TP-LINK®

User Guide

TD-VG3631

300Mbps Wireless N VoIP ADSL2+ Modem Router

Rev: 1.0.0
1910010643

COPYRIGHT & TRADEMARKS

Specifications are subject to change without notice. TP-LINK® is a registered trademark of TP-LINK TECHNOLOGIES CO., LTD. Other brands and product names are trademarks or registered trademarks of their respective holders.

No part of the specifications may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from TP-LINK TECHNOLOGIES CO., LTD. Copyright © 2012 TP-LINK TECHNOLOGIES CO., LTD. All rights reserved.

http://www.tp-link.com

FCC STATEMENT

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/ TV technician for help.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

1) This device may not cause harmful interference.
2) This device must accept any interference received, including interference that may cause undesired operation.

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Note: The manufacturer is not responsible for any radio or tv interference caused by unauthorized modifications to this equipment. Such modifications could void the user's authority to operate the equipment.

FCC RF Radiation Exposure Statement

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter.

"To comply with FCC RF exposure compliance requirements, this grant is applicable to only Mobile Configurations. The antennas used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter."

CE Mark Warning

This is a class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

National Restrictions

This device is intended for home and office use in all EU countries (and other countries following the EU directive 1999/5/EC) without any limitation except for the countries mentioned below:

Country	Restriction	Reason/remark
Bulgaria	None	General authorization required for outdoor use and public service
France	Outdoor use limited to 10 mW e.i.r.p. within the band 2454-2483.5 MHz	Military Radiolocation use. Refarming of the 2.4 GHz band has been ongoing in recent years to allow current relaxed regulation. Full implementation planned 2012
Italy	None	If used outside of own premises, general authorization is required
Luxembourg	None	General authorization required for network and service supply(not for spectrum)
Norway	Implemented	This subsection does not apply for the geographical area within a radius of 20 km from the centre of Ny-Ålesund
Russian Federation	None	Only for indoor applications

Note: Please don’t use the product outdoors in France.

This device has been designed to operate with the antennas listed below, and having a maximum gain of 3 dBi. Antennas not included in this list or having a gain greater than 3 dBi are strictly prohibited for use with this device. The required antenna impedance is 50 ohms.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that permitted for successful communication.

Industry Canada Statement:

This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions:

(1)This device may not cause harmful interference, and

(2)This device must accept any interference received, including interference that may cause undesired operation.

IMPORTANT NOTE:

Radiation Exposure Statement:

This equipment complies with Canada radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

Ce dispositif est conforme à la norme CNR-210 d'Industrie Canada applicable aux appareils radio exempts de licence. Son fonctionnement est sujet aux deux conditions suivantes:

(1) Le dispositif ne doit pas produire de brouillage préjudiciable, et

(2) Ce dispositif doit accepter tout brouillage reçu,y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

NOTE IMPORTANTE:

Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

Korea Warning Statements:

당해 무선설비는 운용중 전파혼신 가능성이 있음.

NCC Notice:

經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前項合法通信，指依電信法規定作業之無線電通信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

Продукт сертифіковано згідно с правилами системи УкрСЕПРО на відповідність вимогам нормативних документів та вимогам, що передбачені чинними законодавчими актами України.

DECLARATION OF CONFORMITY

For the following equipment:

Product Description: **300Mbps Wireless N VoIP ADSL2+ Modem Router**

Model No.: **TD-VG3631**

Trademark: **TP-LINK**

We declare under our own responsibility that the above products satisfy all the technical regulations applicable to the product within the scope of Council Directives:

Directives 1999/5/EC, Directives 2004/108/EC, Directives 2006/95/EC, Directives 1999/519/EC, Directives 2011/65/EU

The above product is in conformity with the following standards or other normative documents

ETSI EN 300 328 V1.7.1: 2006

ETSI EN 301 489-1 V1.8.1:2008& ETSI EN 301 489-17 V2.1.1:2009

EN 55022:2010

EN 55024:2010

EN 61000-3-2:2006+A1:2009+A2:2009

EN 61000-3-3:2008

EN60950-1:2006+A11：2009+A1:2010+A12:2011

EN62311:2008

The product carries the CE Mark:

CE 1588 ⓘ

Person is responsible for marking this declaration:

Yang Hongliang

Product Manager of International Business

Date of issue: 2012

TP-LINK TECHNOLOGIES CO., LTD

Building 24 (floors 1, 3, 4, 5), and 28 (floors 1-4) Central Science and Technology Park, Shennan Rd, Nanshan, Shenzhen, China

CONTENTS

Package Contents **1**

Chapter 1. Product Overview **2**

1.1 Overview of the Modem Router 2

1.2 Main Features 3

1.3 Panel Layout 4

1.3.1 The Front Panel 4

1.3.2 The Back Panel 6

Chapter 2. Connecting the Modem Router **8**

2.1 System Requirements 8

2.2 Installation Environment Requirements 8

2.3 Connecting the Modem Router 8

Chapter 3. Quick Installation Guide **10**

3.1 Configuring the PC 10

3.2 Quick Installation Guide 13

Chapter 4. Configuring the Modem Router **19**

4.1 Login 19

4.2 Status 19

4.3 Quick Setup 20

4.4 Network 20

4.4.1 WAN Settings 21

4.4.2 EWAN 30

4.4.3 Interface Grouping 33

4.4.4 LAN Settings 34

4.4.5 MAC Clone 36

4.4.6 ALG Settings 36

4.4.7 DSL Settings 37

4.5 DHCP Server 38

4.5.1 DHCP Settings 38

4.5.2 Clients List 40

4.5.3 Address Reservation 40

4.5.4 Conditional Pool 41

4.6 Wireless 43
4.6.1 Basic Settings 43
4.6.2 WPS Settings 45
4.6.3 Wireless Security 47
4.6.4 Wireless MAC Filtering 49
4.6.5 Wireless Advanced 50
4.6.6 Wireless Status 52
4.7 Voice 52
4.7.1 SIP Account 52
4.7.2 Dial Plan 54
4.7.3 Phone Setup 57
4.7.4 Advanced Setup 60
4.7.5 Speed Dial 62
4.7.6 Call Log 62
4.7.7 Call Firewall 63
4.7.8 USB Voice Mail 65
4.8 USB Settings 68
4.8.1 USB Mass Storage 68
4.8.2 User Accounts 69
4.8.3 Storage Sharing 70
4.8.4 FTP Server 72
4.8.5 Media Server 74
4.8.6 Print Server 75
4.9 Route Settings 76
4.9.1 Default Gateway 76
4.9.2 Static Route 76
4.9.3 RIP Settings 77
4.10 Forwarding 78
4.10.1 Virtual Servers 78
4.10.2 Port Triggering 79
4.10.3 DMZ 81
4.10.4 UPnP 82
4.11 Parental Control 83
4.12 Firewall 84
4.12.1 Rule 84
4.12.2 LAN Host 85

4.12.3 WAN Host 86
4.12.4 Schedule 88
4.13 Traffic Control 89
4.13.1 Control Settings 89
4.13.2 Rules List 89
4.14 IP&MAC Binding 90
4.14.1 Binding Settings 91
4.14.2 ARP List 92
4.15 Dynamic DNS 92
4.16 Diagnostic 93
4.17 System Tools 94
4.17.1 System Log 94
4.17.2 Time Settings 95
4.17.3 Manage Control 96
4.17.4 CWMP Settings 96
4.17.5 SNMP Settings 97
4.17.6 Backup & Restore 98
4.17.7 Factory Defaults 98
4.17.8 Firmware Upgrade 99
4.17.9 Reboot 100
4.17.10 Statistics 100
Appendix A: Specifications 102
Appendix B: Troubleshooting 103
Appendix C: Telephony Features 112
Appendix D: Telephone Operation 114
Appendix E: Technical Support 116

Package Contents

The following contents should be found in your package:

- One TD-VG3631 300Mbps Wireless N VoIP ADSL2+ Modem Router
- One Power Adapter for TD-VG3631 300Mbps Wireless N VoIP ADSL2+ Modem Router
- Quick Installation Guide
- One RJ45 cable
- Three RJ11 cables
- One ADSL splitter
- One Resource CD for TD-VG3631 300Mbps Wireless N VoIP ADSL2+ Modem Router, including:
  - This User Guide
  - Other Helpful Information

☞ **Note:**

Make sure that the package contains the above items. If any of the listed items are damaged or missing, please contact your distributor.

Chapter 1. Product Overview

Thank you for choosing the **TD-VG3631 300Mbps Wireless N VoIP ADSL2+ Modem Router**.

1.1 Overview of the Modem Router

The TD-VG3631 300Mbps Wireless N VoIP ADSL2+ Modem Router integrates 4-port Switch, Firewall, NAT-Router and Wireless AP. Powered by 2x2 MIMO technology, the Wireless N Router delivers exceptional range and speed, which can fully meet the need of Small Office/Home Office (SOHO) networks and the users demanding higher networking performance.

The TD-VG3631 300Mbps Wireless N VoIP ADSL2+ Modem Router utilizes integrated ADSL2+ transceiver and high speed MIPS CPU. The Router supports full-rate ADSL2+ connectivity conforming to the ITU and ANSI specifications.

In addition to the basic DMT physical layer functions, the ADSL2+ PHY supports dual latency ADSL2+ framing (fast and interleaved) and the I.432 ATM Physical Layer.

The router provides up to 300Mbps wireless connection with other 802.11n wireless clients. The incredible speed makes it ideal for handling multiple data streams at the same time, which ensures your network stable and smooth. The performance of this 802.11n wireless Router will give you the unexpected networking experience at speed 650% faster than 802.11g. It is also compatible with all IEEE 802.11g and IEEE 802.11b products.

With multiple protection measures, including SSID broadcast control and wireless LAN 64/128 WEP encryption, Wi-Fi protected Access (WPA2-PSK, WPA-PSK), as well as advanced Firewall protections, the TD-VG3631 300Mbps Wireless N VoIP ADSL2+ Modem Router provides complete data privacy.

The Router provides flexible access control, so that parents or network administrators can establish restricted access policies for children or staff. It also supports Virtual Server and DMZ host for Port Triggering, and then the network administrators can manage and monitor the network in real time with the remote management function.

Since the Router is compatible with virtually all the major operating systems, it is very easy to manage. Quick Setup Wizard is supported and detailed instructions are provided step by step in this user guide. Before installing the Router, please look through this guide to know all the Router's functions.

1.2 Main Features

- Four 10/100Mbps Auto-Negotiation RJ45 LAN ports (Auto MDI/MDIX), four RJ11 ports, two USB 2.0 ports
- Provides external splitter.
- Adopts Advanced DMT modulation and demodulation technology.
- Supports bridge mode and Router function.
- Multi-user sharing a high-speed Internet connection.
- Downstream data rates up to 24Mbps, upstream data rates up to 3.5Mbps (With Annex M enabled).
- Supports long transfers, the max line length can reach to 6.5Km.
- Supporting both traditional land lines and VoIP network offers you a multiple choice when making phone calls
- Various call features such as Multi-accounts, call waiting, call holding, call forwarding, 3-way conference calls and USB voice mail
- Supports remote configuration and management through SNMP and CWMP.
- Supports PPPoE, it allows connecting the internet on demand and disconnecting from the Internet when idle.
- Provides reliable ESD and surge-protect function with quick response semi-conductive surge protection circuit.
- High speed and asymmetrical data transmit mode, provides safe and exclusive bandwidth.
- Supports All ADSL industrial standards.
- Compatible with all mainstreams DSLAM (CO).
- Provides integrated access of internet and route function which face to SOHO user.
- Real-time Configuration and device monitoring.
- Supports Multiple PVC (Permanent Virtual Circuit).
- Built-in DHCP server.
- Built-in firewall, supporting IP/MAC filter, Application filter and URL filter.
- Supports Virtual Server, DMZ host and IP Address Mapping.
- Supports Dynamic DNS, UPnP and Static Routing.
- Supports system log and flow Statistics.
- Supports firmware upgrade and Web management.
- Provides WPA-PSK/WPA2-PSK data security, TKIP/AES encryption security.
- Provides 64/128-bit WEP encryption security and wireless LAN ACL (Access Control List).
- Supports USB Storage Sharing, Print Server, FTP Server, Media Server.
- Supports Ethernet WAN (EWAN).
- Supports Bandwidth Control.

1.3 Panel Layout

1.3.1 The Front Panel

Figure 1-1

The Router's LEDs are located on the front panel (View from left to right). They indicate the device's working status. For details, please refer to LED Explanation.

LED Explanation:

Name	Status	Indication
(Power)	On	The modem router is powered on.
	Off	The modem router is off. Please ensure that the power adapter is connected correctly.
(ADSL)	On	ADSL line is synchronized and ready to use.
	Flash	The ADSL negotiation is in progress.
	Off	ADSL synchronization fails. Please refer to Note 1 for troubleshooting.
(Internet)	On	The network is available with a successful Internet connection.
	Flash	There is data being transmitted or received via the Internet.
	Off	There is no successful Internet connection or the modem router is operating in Bridge mode. Please refer to Note 2 for troubleshooting.
(WLAN)	On	Wireless is enabled but no data is being transmitted.
	Flash	The modem router is sending or receiving data over the wireless network.
	Off	Wireless function is disabled.
(LAN1-4)	On	There is a device connected to this LAN port.
	Flash	The modem router is sending or receiving data over this LAN port.
	Off	There is no device connected to this LAN port.
(USB)	On	A storage device or printer has connected to the USB port.
	Flash	The modem router is sending or receiving data over this USB port.
	Off	No storage device or printer is plugged into the USB port.

（Line）	On	A valid PSTN connection.
	Flash	Incoming calls and outgoing calls are transmitted trough PSTN line.
	Off	PSTN connection fails.
（Phone1-2）	On	The phone is off hook.
	Flash	The phone is ringing.
	Off	The phone is on hook.
(WPS)	On	A wireless device has been successfully added to the network by WPS function.
	Slow Flash	WPS handshaking is in process and will continue for about 2 minutes. Please press the WPS button on other wireless devices that you want to add to the network while the LED is flashing.
	Quick Flash	A wireless device has failed to be added to the network by WPS function. Please refer to 4.6.2 WPS Settings for more information.

☞ **Note:**

1. If the ADSL LED is off, please check your Internet connection first. Refer to **2.3 Connecting the Modem Router** for more information about how to make Internet connection correctly. If you have already made a right connection, please contact your ISP to make sure if your Internet service is available now.
2. If the Internet LED is off, please check your ADSL LED first. If your ADSL LED is also off, please refer to **Note 1**. If your ADSL LED is GREEN ON, please check your Internet configuration. You may need to check this part of information with your ISP and make sure everything have been input correctly.

1.3.2 The Back Panel

The Router's ports, where the cables are connected, and RESET button are located on the front

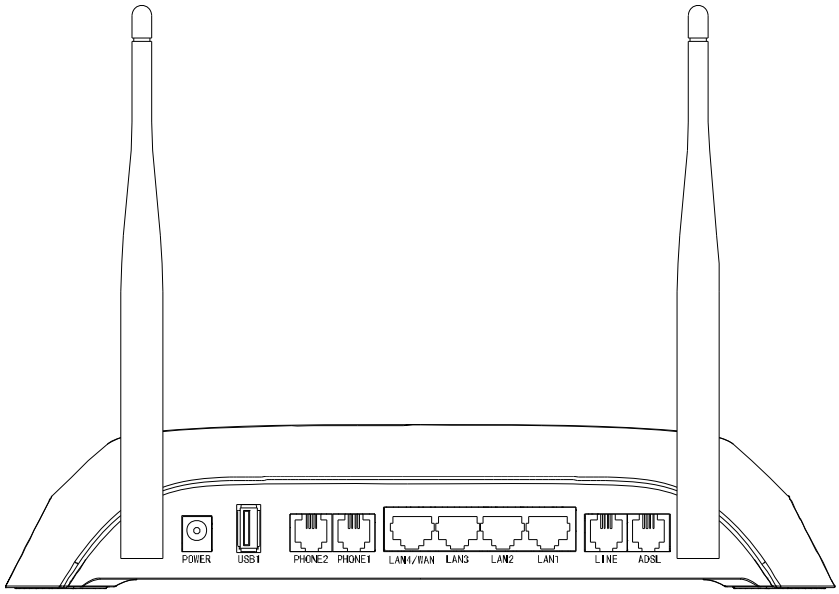


Figure 1-2

- **POWER:** The Power plug is where you will connect the power adapter.
- **USB1/USB2:** The USB port connects to a USB storage device or a USB printer.
- **PHONE2/PHONE1:**The phone port connects to a phone set.
- **LAN1, LAN2, LAN3, LAN4/WAN:** Through these ports, you can connect the Router to your PC or the other Ethernet network devices. Enable EWAN function and you will be able to connect to Cable/FTTH/VDSL/ADSL device.
- **LINE:** Connect this port to PSTN phone cable. Or you can connect them by an external separate splitter. For details, please refer to 2.3 Connecting the Router.
- **ADSL:** Through the port, you can connect the Modem Router with the telephone. Or you can connect them by an external separate splitter. For details, please refer to 2.3 Connecting the Router.
- **Antennas:** Used for wireless operation and data transmit.
- **RESET:** There are two ways to reset the Router's factory defaults.

  Method one: With the Router powered on, use a pin to press and hold the Reset button for at least 5 seconds. And the Router will reboot to its factory default settings.

  Method two: Restore the default setting from “Maintenance-SysRestart” of the Router's Web-based Utility.

Ports and buttons on the left side

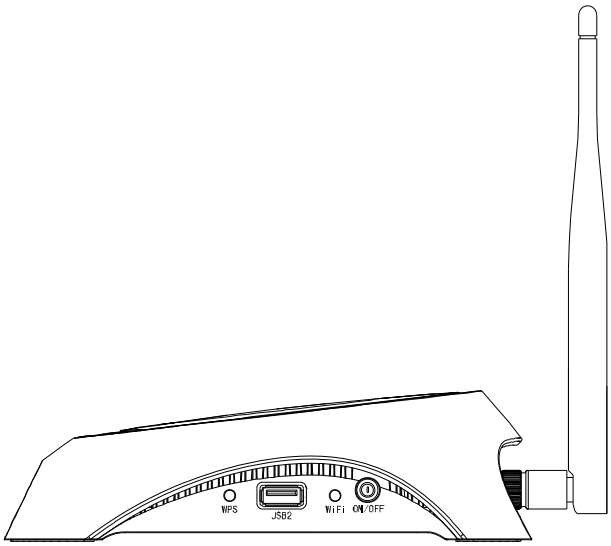


Figure 1-3

- **WPS**: The switch for the WPS function. For details, please refer to 4.6.2 WPS Settings.
- **WiFi**: The switch for the WiFi function.
- **ON/OFF**: The switch for the power.

Chapter 2. Connecting the Modem Router

2.1 System Requirements

- Broadband Internet Access Service (DSL/Cable/Ethernet).
- PCs with a working Ethernet Adapter and an Ethernet cable with RJ45 connectors.
- TCP/IP protocol on each PC.
- Web browser, such as Microsoft Internet Explorer, Mozilla Firefox or Apple Safari.

2.2 Installation Environment Requirements

- The Product should not be located where it will be exposed to moisture or excessive heat.
- Place the Router in a location where it can be connected to the various devices as well as to a power source.
- Make sure the cables and power cord are safely placed out of the way so they do not create a tripping hazard.
- The Router can be placed on a shelf or desktop.
- Keep away from the strong electromagnetic radiation and the device of electromagnetic sensitive.

2.3 Connecting the Modem Router

Before installing the device, please make sure your broadband service provided by your ISP is available. If there is any problem, please contact your ISP. Before cable connection, cut off the power supply and keep your hands dry. You can follow the steps below to install it.

Step 1: Connect the ADSL Line. You can use a separate splitter. External splitter can divide the data and voice, and then you can access the Internet and make calls at the same time. The external splitter has three ports:

- LINE: Connect to the wall jack
- PHONE: Connect to the LINE port of the Modem Router
- MODEM: Connect to the ADSL port of the Modem Router

Step 2: Connect the Ethernet cable. Attach one end of a network cable to your computer's Ethernet port or a regular hub/switch port, and the other end to the LAN port on the Modem Router.

Step 3: Connect your telephone to the Port labeled "PHONE 1~2" on the Modem Router with a telephone line.

Step 4: Power on the computers and LAN devices.

Step 5: Attach the power adapter. Connect the power adapter to the power connector on the rear of the device and plug in the adapter to an electrical outlet or power extension. The electrical outlet shall be installed near the device and shall be easily accessible.

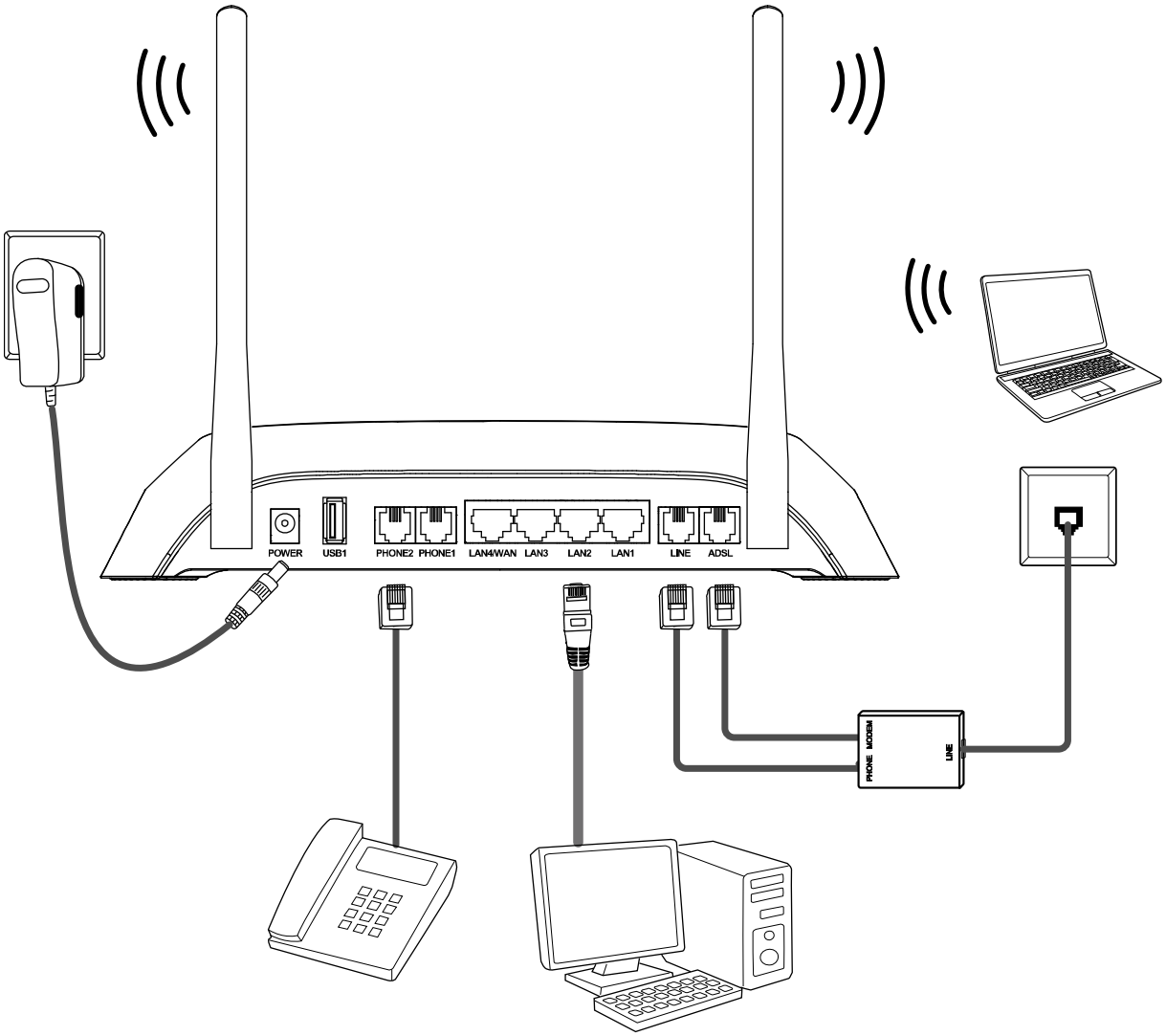

POWER
USB1
PHONE2
PHONE1
LAN4/WAN
LAN3
LAN2
LAN1
LINE
ADSL
PHONE
MODEM
LINE

Figure 2-1

Chapter 3. Quick Installation Guide

3.1 Configuring the PC

After you directly connect your PC to the Modem Router or connect your adapter to a Hub/Switch which has connected to the Modem Router, you need to configure your PC's IP address. Follow the steps below to configure it.

Step 1: Click the **Start** menu on your desktop, right click **My Network Places**, and then select **Properties** (shown in Figure 3-1).

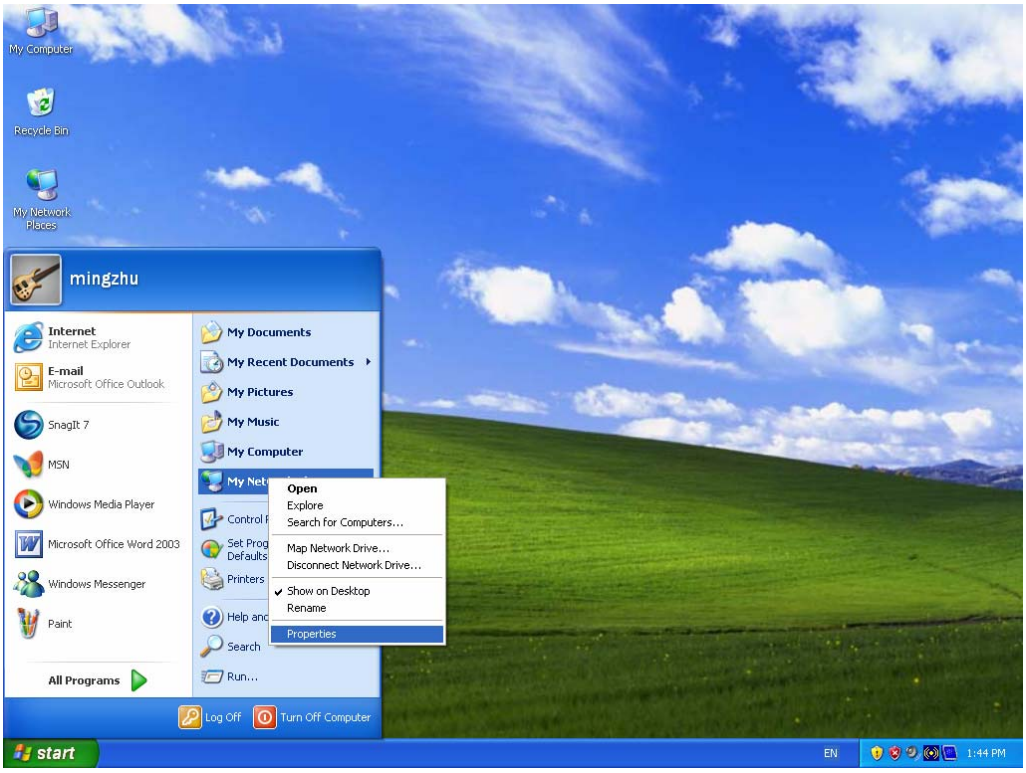


Figure 3-1

Step 2: Right click **Local Area Connection** (LAN), and then select **Properties**.

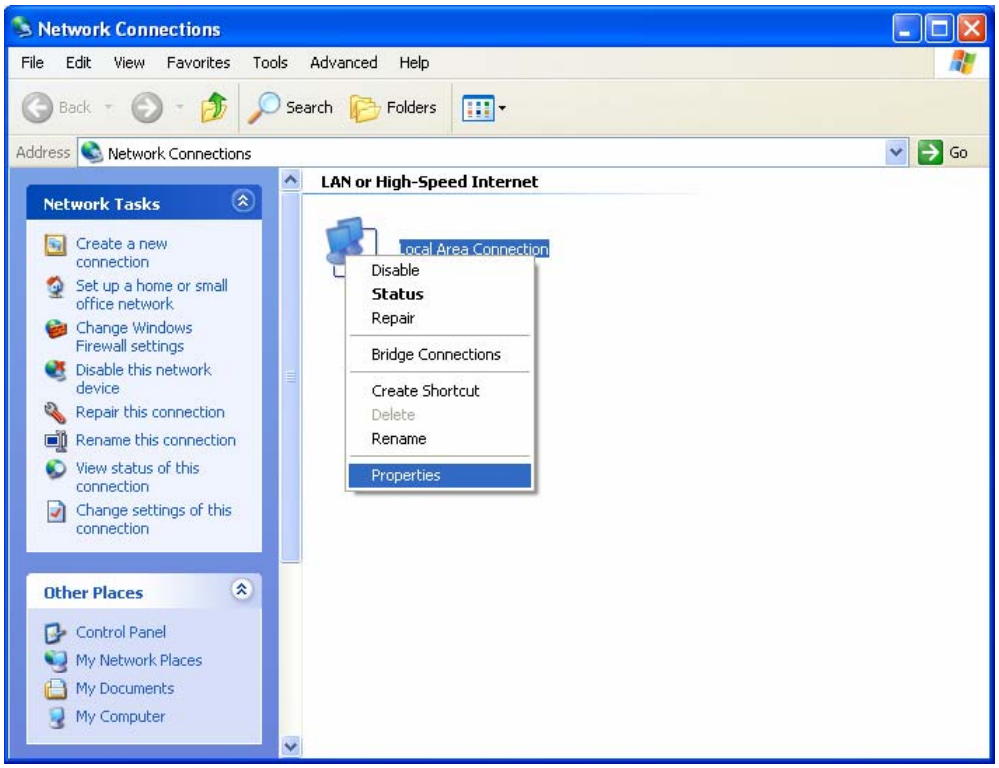


Figure 3-2

Step 3: Select **General** tab, highlight **Internet Protocol (TCP/IP)**, and then click the **Properties** button.

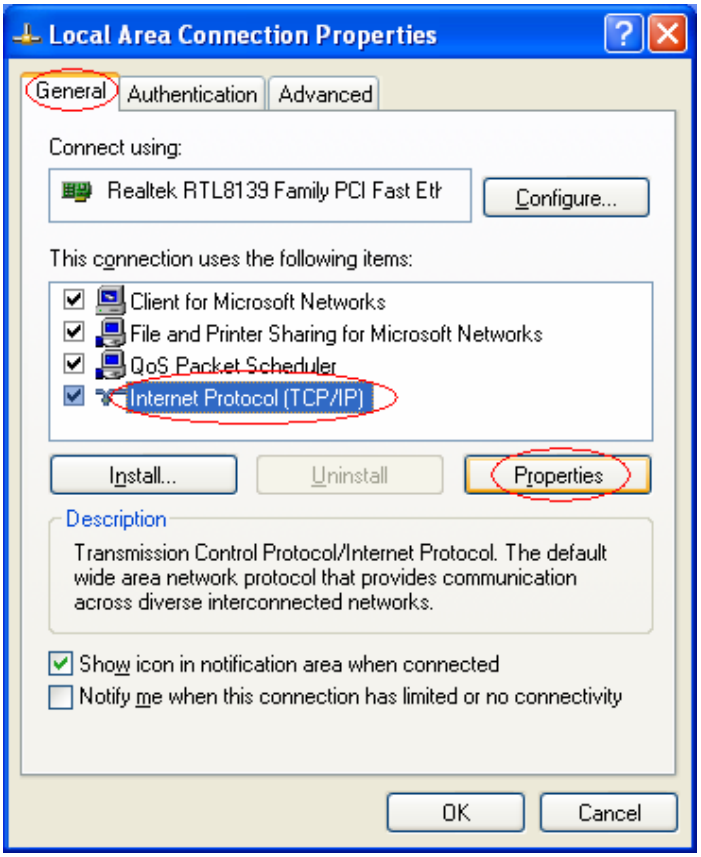


Figure 3-3

Step 4: Configure the IP address as Figure 3-4 shows. After that, click **OK**.

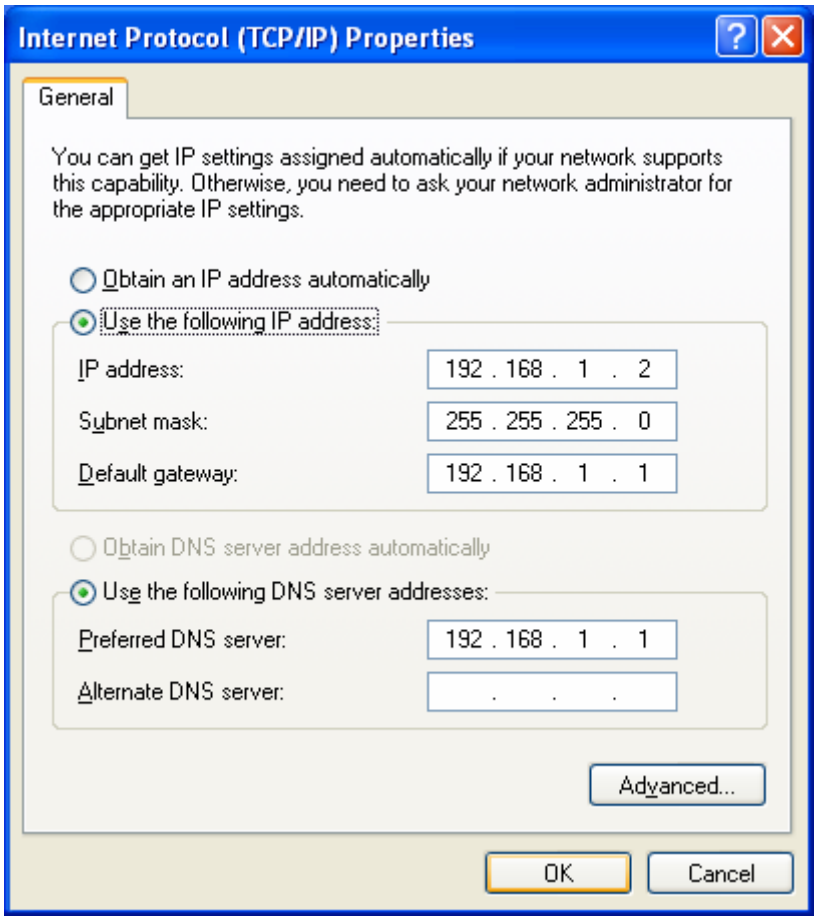

Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 192 . 168 . 1 . 2
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 1 . 1
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server: 192 . 168 . 1 . 1
Alternate DNS server:
Advanced...
OK
Cancel

Figure 3-4

Note:

You can configure the PC to get an IP address automatically, select “Obtain an IP address automatically” and “Obtain DNS server address automatically” in the screen above.

Now, you can run the Ping command in the command prompt to verify the network connection. Please click the **Start** menu on your desktop, select **run** tab, type **cmd or command** in the field and press **Enter**. Type ***ping 192.168.1.1*** on the next screen, and then press **Enter**.

If the result displayed is similar to the screen below, the connection between your PC and the Modem Router has been established.

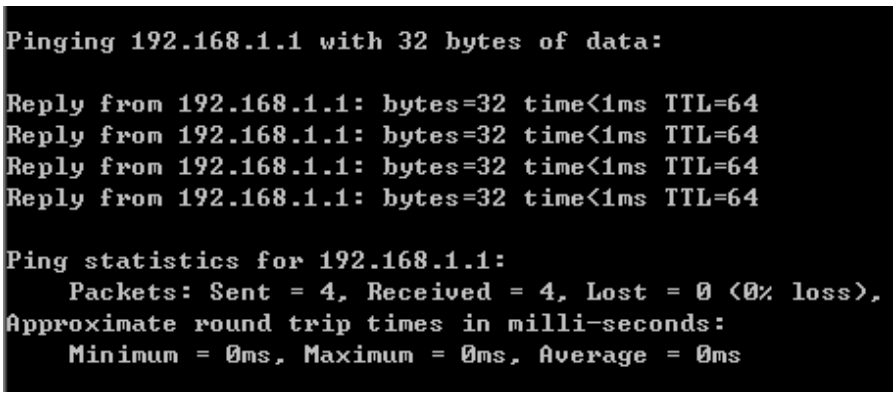

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Ping statistics for 192.168.1.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms

Figure 3-5

If the result displayed is similar to the screen shown below, it means that your PC has not connected to the Modem Router.

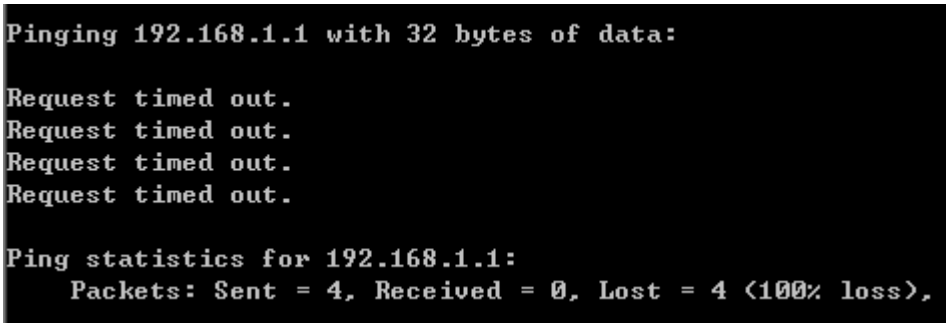

Pinging 192.168.1.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.1.1:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

Figure 3-6

You can check it following the steps below:

1) Is the connection between your PC and the Modem Router correct?

The LEDs of LAN port which you link to the device and the LEDs on your PC's adapter should be lit.

2) Is the TCP/IP configuration for your PC correct?

If the Router's IP address is 192.168.1.1, your PC's IP address must be within the range of 192.168.1.2 ~ 192.168.1.254.

3.2 Quick Installation Guide

With a Web-based utility, it is easy to configure and manage the TD-VG3631 300Mbps Wireless N VoIP ADSL2+ Modem Router. The Web-based utility can be used on any Windows, Macintosh or UNIX OS with a Web browser, such as Microsoft Internet Explorer, Mozilla Firefox or Apple Safari.

1. To access the configuration utility, open a web-browser and type the default address http://192.168.1.1 in the address field of the browser.

Figure 3-7

After a moment, a login window will appear, similar to the Figure 3-8. Enter **admin** for the User Name and Password, both in lower case letters. Then click the **OK** button or press the **Enter** key.

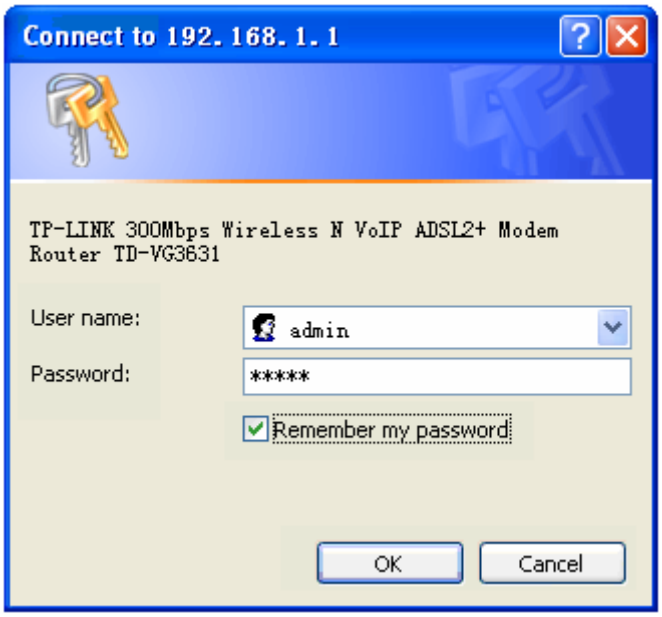


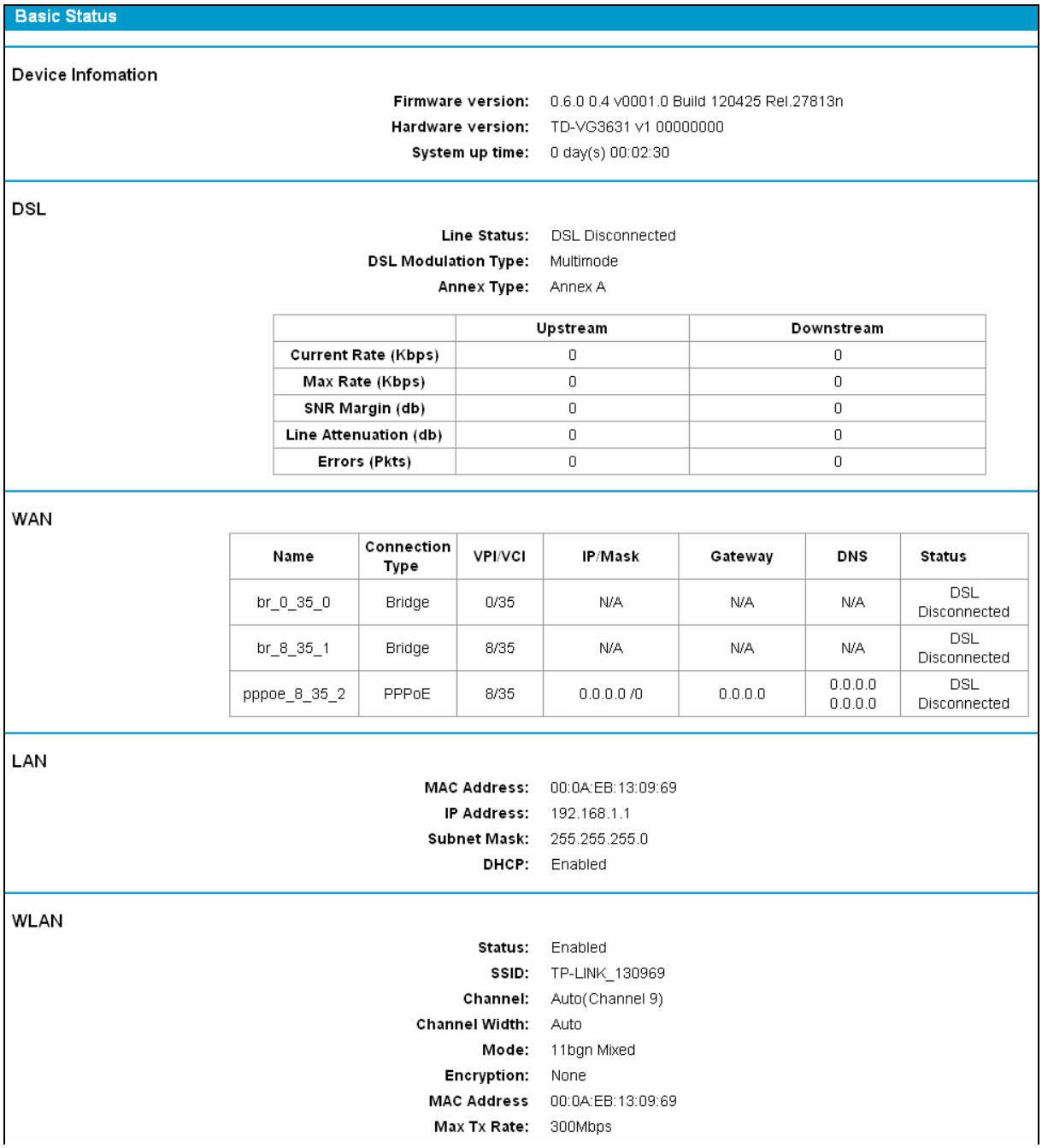
Figure 3-8

☞ **Note:**

1) Do not mix up the user name and password with your ADSL account user name and password which are needed for PPP connections.

2) If the above screen does not pop up, it means that your Web-browser has been set to a proxy. Go to **Tools** menu→**Network**→**LAN Settings**, in the screen that appears, cancel the Using Proxy checkbox, and click **OK** to finish it.

2. After your successful login, you will see the Login screen as shown in Figure 3-9. Click **Quick Setup** menu to access **Quick Setup Wizard**.



Basic Status

Device Infomation

Firmware version:	0.6.0 0.4 v0001.0 Build 120425 Rel.27813n
Hardware version:	TD-VG3631 v1 00000000
System up time:	0 day(s) 00:02:30

DSL

Line Status:	DSL Disconnected
DSL Modulation Type:	Multimode
Annex Type:	Annex A

	Upstream	Downstream
Current Rate (Kbps)	0	0
Max Rate (Kbps)	0	0
SNR Margin (db)	0	0
Line Attenuation (db)	0	0
Errors (Pkts)	0	0

WAN

Name	Connection Type	VPI/VCI	IP/Mask	Gateway	DNS	Status
br_0_35_0	Bridge	0/35	N/A	N/A	N/A	DSL Disconnected
br_8_35_1	Bridge	8/35	N/A	N/A	N/A	DSL Disconnected
pppoe_8_35_2	PPPoE	8/35	0.0.0.0 /0	0.0.0.0	0.0.0.0 0.0.0.0	DSL Disconnected

LAN

MAC Address:	00:0A:EB:13:09:69
IP Address:	192.168.1.1
Subnet Mask:	255.255.255.0
DHCP:	Enabled

WLAN

Status:	Enabled
SSID:	TP-LINK_130969
Channel:	Auto(Channel 9)
Channel Width:	Auto
Mode:	11bgn Mixed
Encryption:	None
MAC Address	00:0A:EB:13:09:69
Max Tx Rate:	300Mbps

Figure 3-9

3. Change the VPI or VCI values which are used to define a unique path for your connection. **If you have been given specific settings for this to configuration, type in the correct values assigned by your ISP.** Click **Next**.

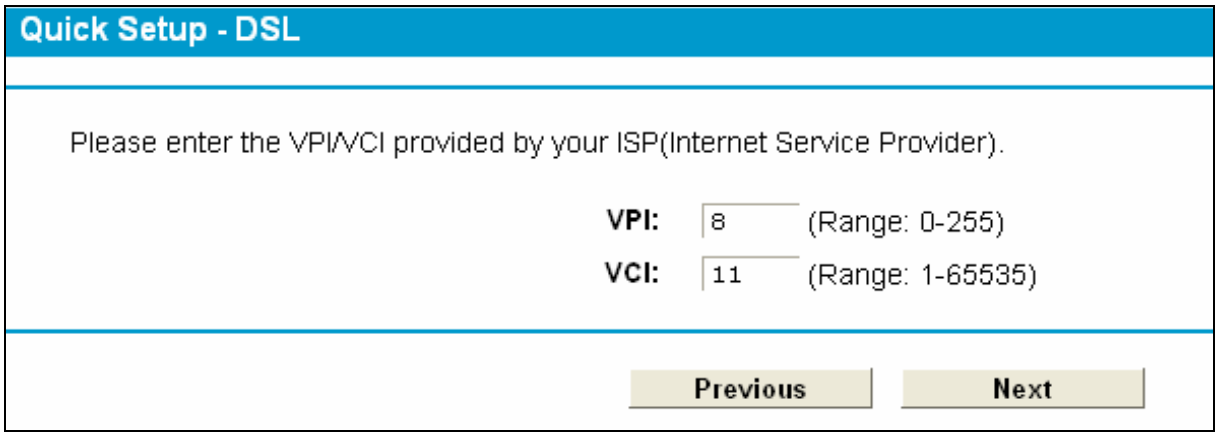


Figure 3-10

4. Here we select PPPoE WAN Link Type for example, enter the **Username**, **Password** and **Confirm Password** given by your ISP, and then click **Next**.

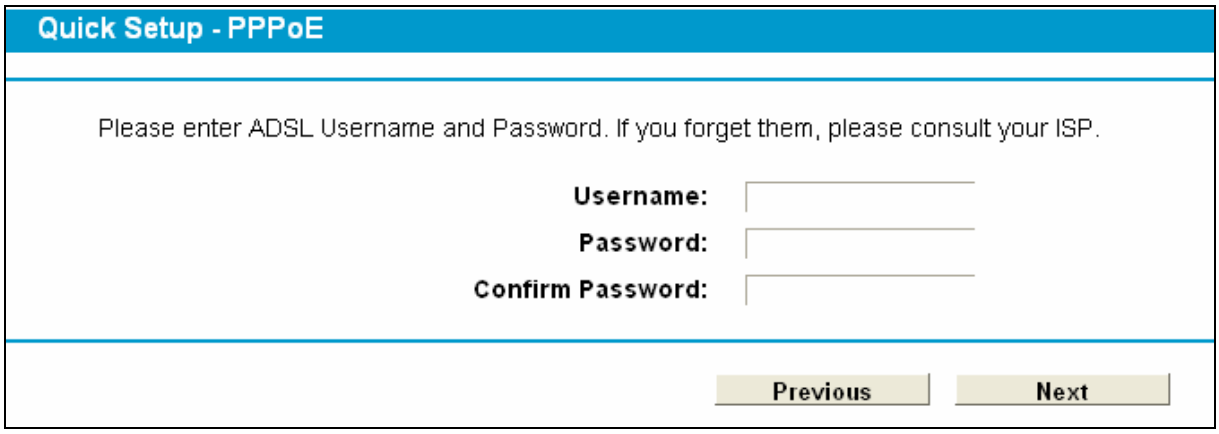


Figure 3-11

5. On the **Wireless** screen, we use the default SSID, select **Region** and **Mode**. Set a Password or select **Disable Security**(**Disable Security** is not recommended.), and then click **Next** to continue.

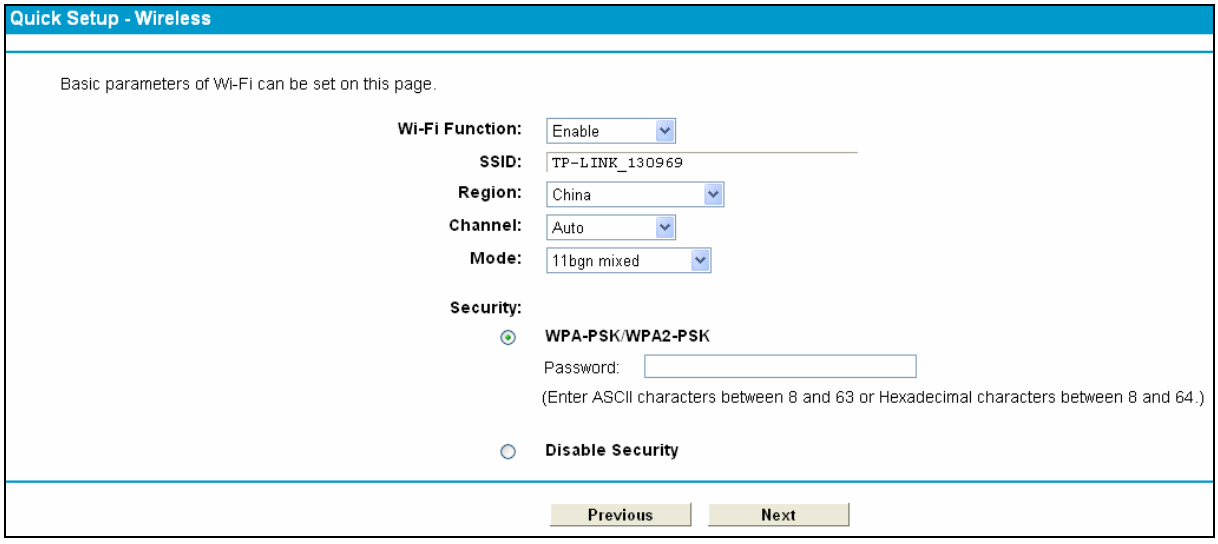


Figure 3-12

6. Basic parameters of Voice can be set on the **Voice** screen. Please enter a profile name to identify this account and other parameters provided by your ISP. If you don't want to configure VoIP function now, leave "Profile Name" blank and click **Next** to skip.

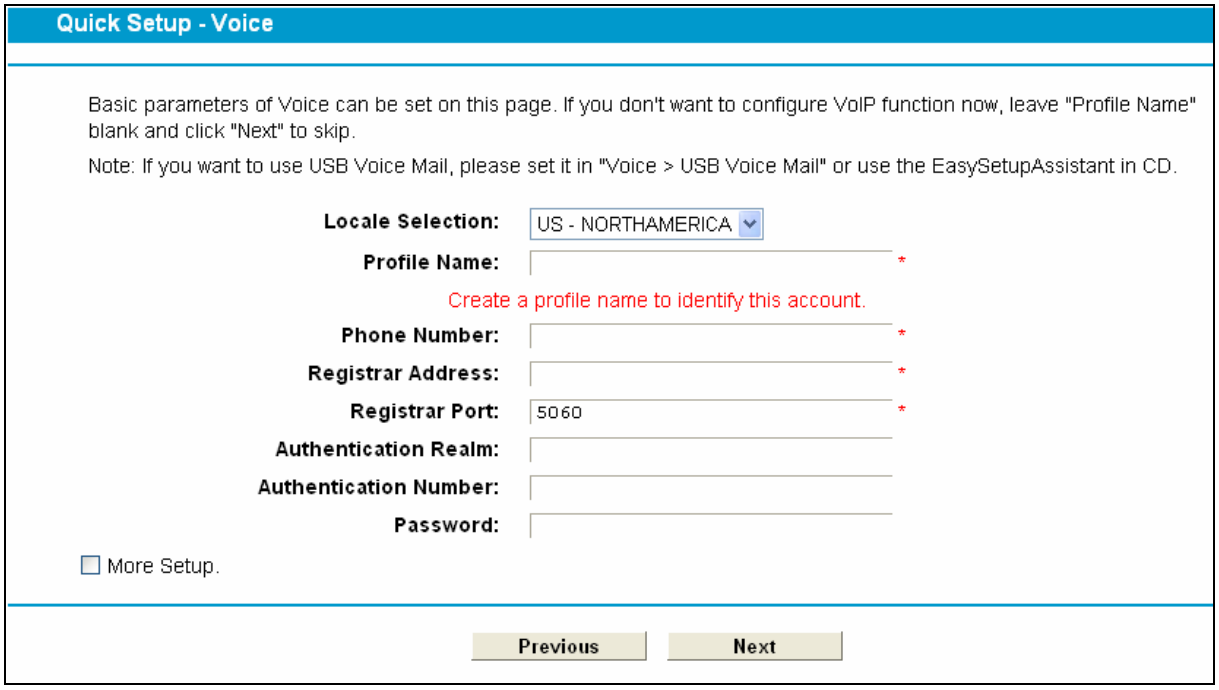

Quick Setup - Voice
Basic parameters of Voice can be set on this page. If you don't want to configure VoIP function now, leave "Profile Name" blank and click "Next" to skip.
Note: If you want to use USB Voice Mail, please set it in "Voice > USB Voice Mail" or use the EasySetupAssistant in CD.
Locale Selection:
US - NORTHAMERICA
Profile Name:
Create a profile name to identify this account.
Phone Number:
Registrar Address:
Registrar Port:
5060
Authentication Realm:
Authentication Number:
Password:
More Setup.
Previous
Next

Figure 3-13

7. On this page, please confirm all parameters. Click **Previous** to modify or click the **Save** button to make the configuration take effect.

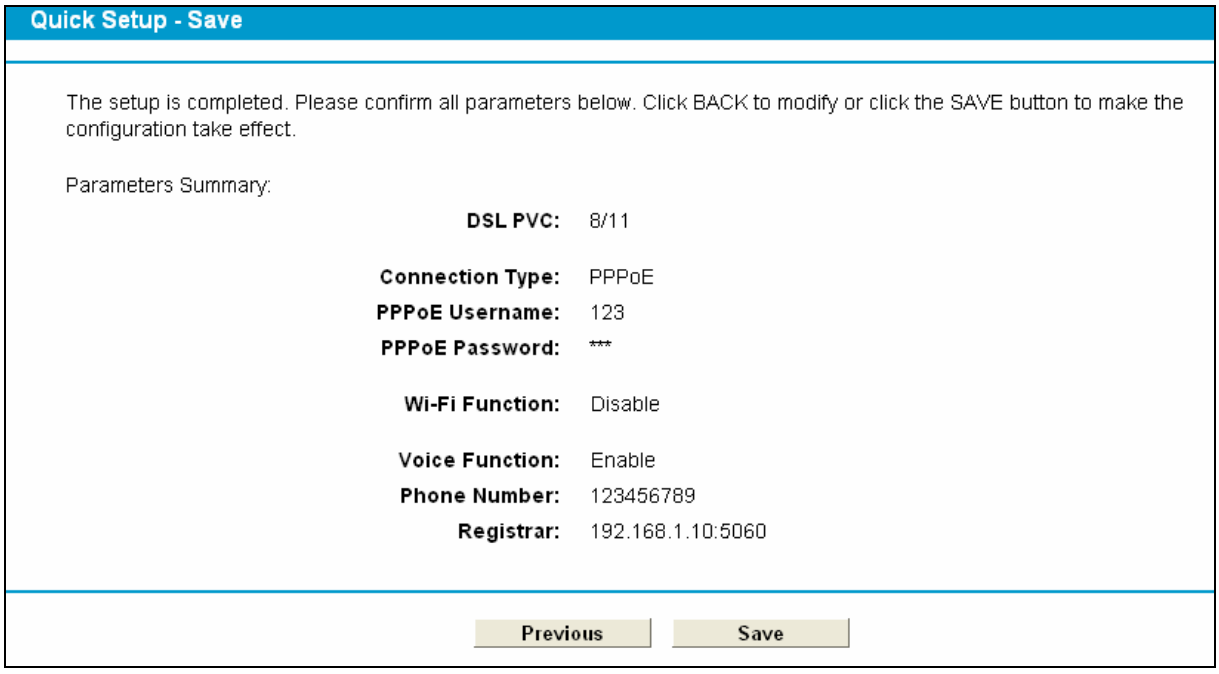

Quick Setup - Save
The setup is completed. Please confirm all parameters below. Click BACK to modify or click the SAVE button to make the configuration take effect.
Parameters Summary:
DSL PVC: 8/11
Connection Type: PPPoE
PPPoE Username: 123
PPPoE Password: ***
Wi-Fi Function: Disable
Voice Function: Enable
Phone Number: 123456789
Registrar: 192.168.1.10:5060
Previous
Save

Figure 3-14

8. You will see the **Complete** screen below, click **Finish** to complete these settings.

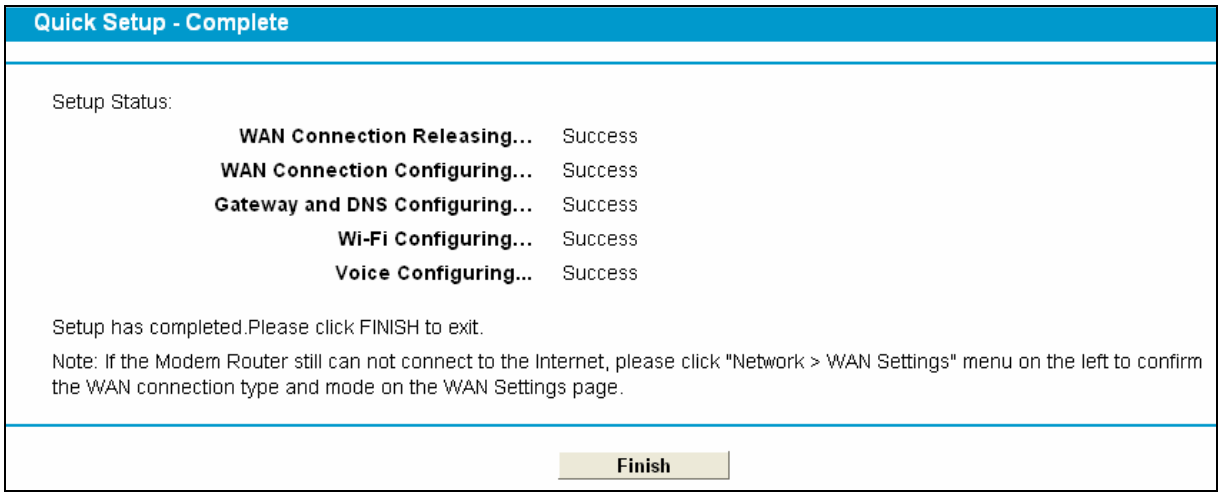

Quick Setup - Complete
Setup Status:
WAN Connection Releasing... Success
WAN Connection Configuring... Success
Gateway and DNS Configuring... Success
Wi-Fi Configuring... Success
Voice Configuring... Success
Setup has completed.Please click FINISH to exit.
Note: If the Modem Router still can not connect to the Internet, please click "Network > WAN Settings" menu on the left to confirm the WAN connection type and mode on the WAN Settings page.
Finish

Figure 3-15

Chapter 4. Configuring the Modem Router

This chapter will show each Web page's key function and the configuration way.

4.1 Login

After your successful login, you will see the fifteen main menus on the left of the Web-based utility. On the right, there are the corresponding explanations and instructions.

The detailed explanations for each Web page's key function are listed below.

4.2 Status

Choose "**Status**", you can see the corresponding information about **Device Information**, **DSL**, **WAN**, **LAN WLAN** and **Voice**.

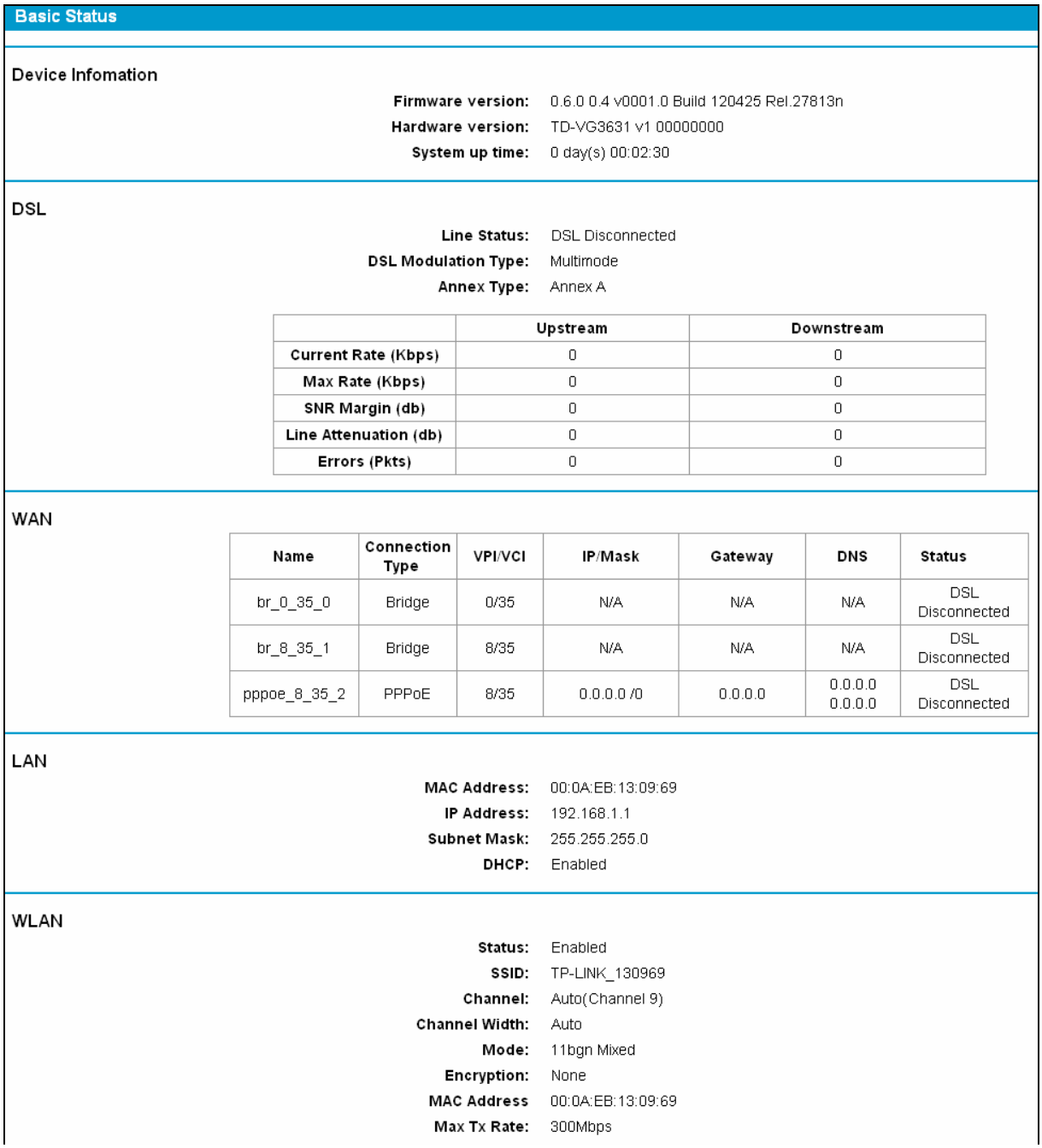


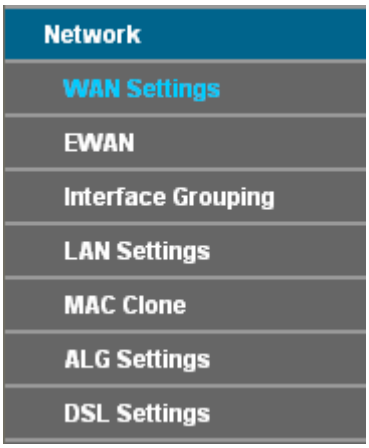
Figure 4-1

4.3 Quick Setup

Please refer to Section 3.2 Quick Installation Guide.

4.4 Network

Choose “**Network**”, there are many submenus under the main menu. Click any one of them, and you will be able to configure the corresponding function.



4.4.1 WAN Settings

Choose "**Network**"→"**WAN Settings**", and you will see the WAN Port Information Table in the screen similar to Figure 4-2, which describes the WAN port settings and the relevant manipulation to each interface. There are five different configurations for the connection types, which are Static IP, Dynamic IP, PPPoE, IPoA, and Bridge. You can select the corresponding types according to your needs.

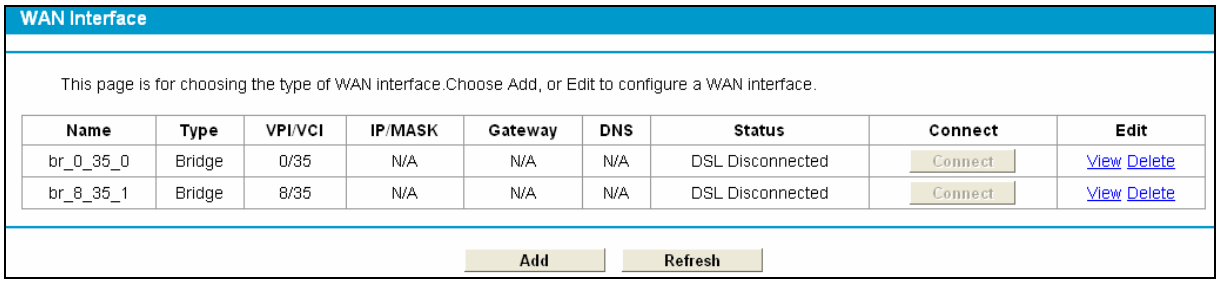

WAN Interface
This page is for choosing the type of WAN interface.Choose Add, or Edit to configure a WAN interface.
Name Type VPI/VCI IP/MASK Gateway DNS Status Connect Edit
br_0_35_0 Bridge 0/35 N/A N/A N/A DSL Disconnected Connect View Delete
br_8_35_1 Bridge 8/35 N/A N/A N/A DSL Disconnected Connect View Delete
Add
Refresh

Figure 4-2

Click **Add** to add a new entry, you can configure the parameters for ATM and WAN Service in the next screen (shown in Figure 4-3).

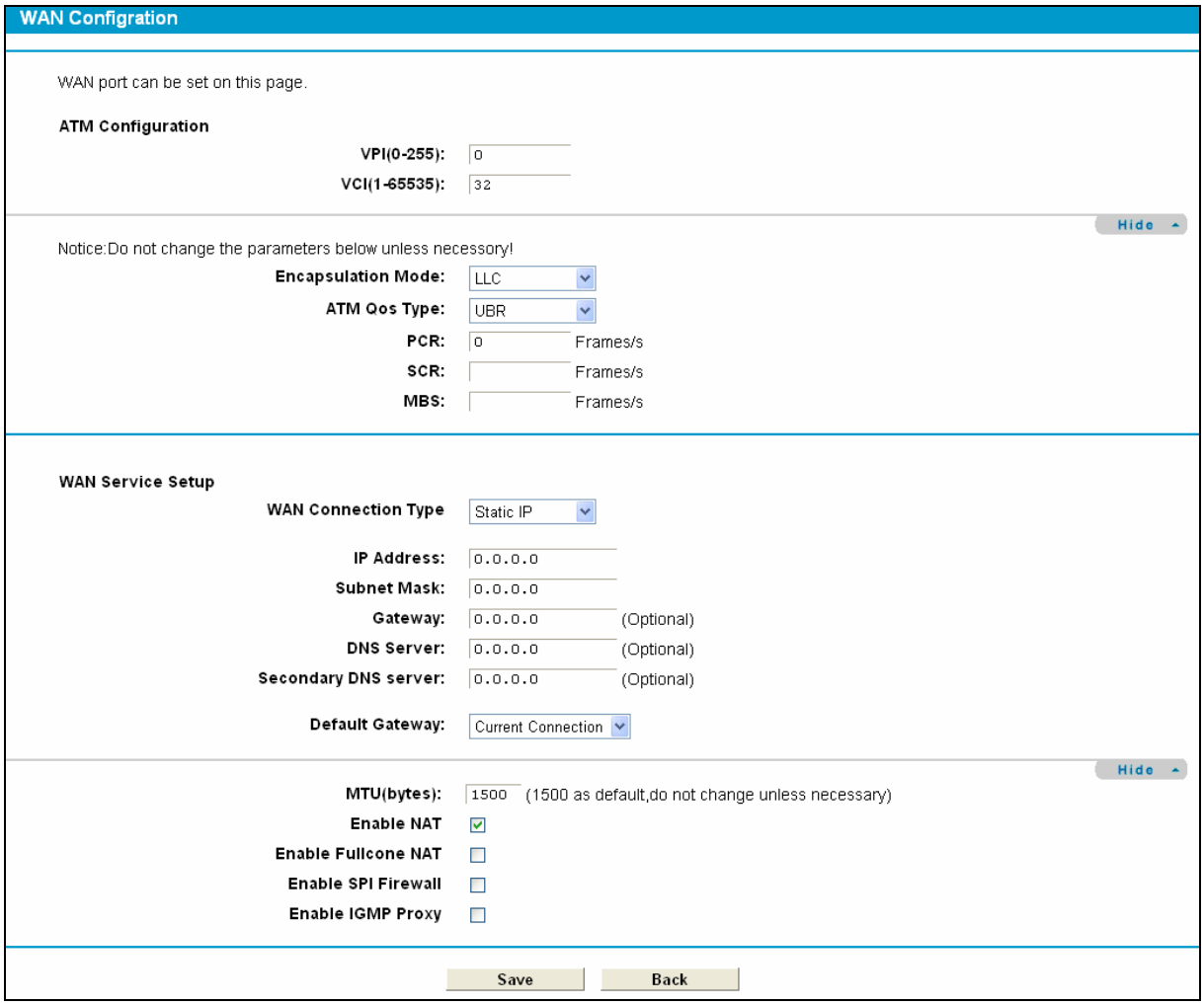


Figure 4-3

4.4.1.1 Static IP

Select this option if your ISP provides static IP information to you. You should set static IP address, IP subnet mask, and gateway address in the screen below.

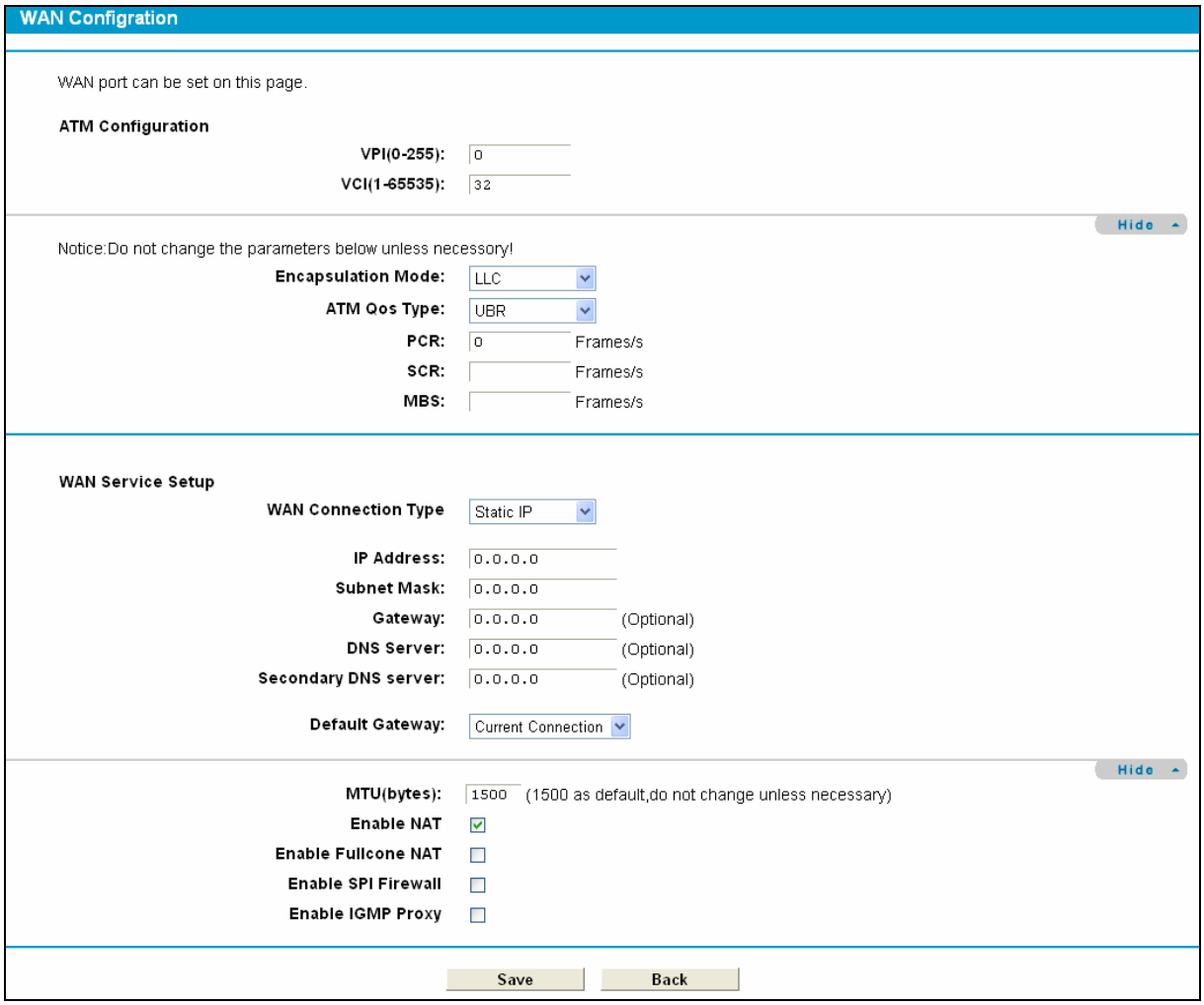


Figure 4-4

ATM Configuration:

- **VPI (0~255):** Identifies the virtual path between endpoints in an ATM network. The valid range is from 0 to 255. Please input the value provided by your ISP.
- **VCI (1~65535):** Identifies the virtual channel endpoints in an ATM network. The valid range is from 1 to 65535 (1 to 31 is reserved for well-known protocols). Please input the value provided by your ISP.

Click **Advanced**, advanced selections of ATM Configuration can be shown.

- **Encapsulation Mode:** Select the encapsulation mode for the Static IP Address. Here you can leave it default.
- **ATM Qos Type:** Select ATM Qos Type provided by ISP, and the type is UBR by default.

WAN Service Setup:

- **IP Address:** Enter the IP address in dotted-decimal notation provided by your ISP.
- **Subnet Mask:** Enter the subnet Mask in dotted-decimal notation provided by your ISP, usually is 255.255.255.0.
- **Default Gateway (Optional):** Enter the gateway IP address in dotted-decimal notation provided by your ISP.

- **DNS Server/ Secondary DNS Server:** Here you can set DNS Server (at least one) manually. The Route will use this DNS Server for priority.
- **Default Gateway:** select a WAN Interface from the drop-down list as the IPv4 default gateway.
- **MTU (bytes):** Maximum Transmission Unit Size. Check this box then you can change the MTU size. The default **MTU** value is 1500 Bytes. It is not recommended that you change the default value unless required by your ISP.
- **Enable NAT:** This technology translates the IP addresses of a local area network to a different IP address for the Internet. If this Modem Router is hosting your network's connection to the Internet, please select the check box. If another Router exists in your network, you don't need to select the option.
- **Enable Fullcone NAT**: It is a type of NAT, if not enabled, the default NAT will act.
- **Enable SPI Firewall:** A SPI firewall enhances network's security. Select the option to use a firewall, or else without a firewall.
- **Enable IGMP Proxy**: IGMP (Internet Group Management Protocol) is used to manage multicasting on TCP/IP networks. Some ISPs use IGMP to perform remote configuration for client devices, such as the Modem Router. The default value is disabled, and if you are not sure, please contact your ISP or just leave it.

Click the **Save** button to save the settings.

4.4.1.2 Dynamic IP

Select this option, the Modem Router will be able to obtain IP network information dynamically from a DHCP server provided by your ISP.

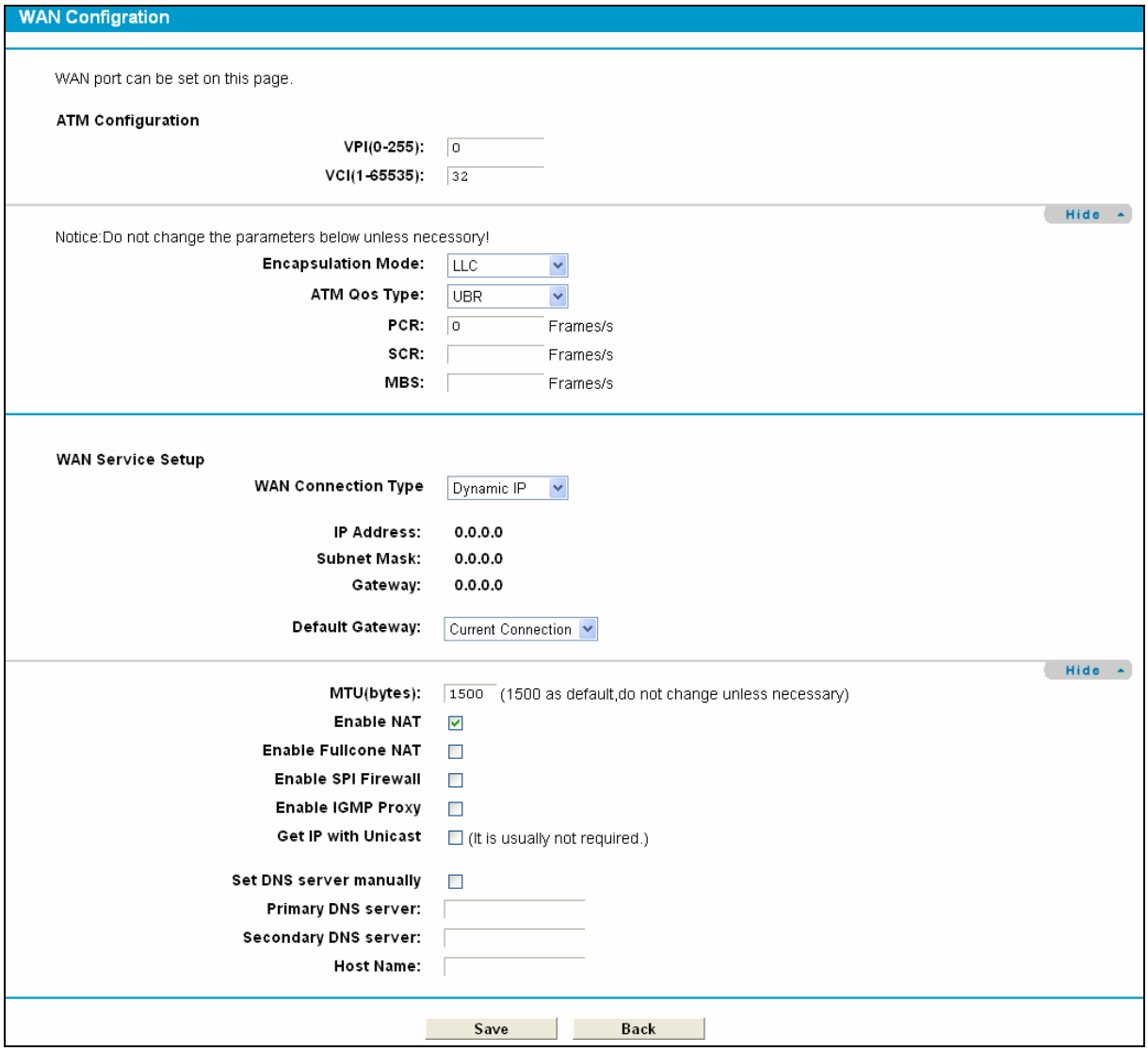


Figure 4-5

Click **Advanced**, advanced selections for WAN Service Setup can be shown.

- **MTU (bytes):** Maximum Transmission Unit Size. Check this box then you can change the MTU size. The default **MTU** value is 1500 Bytes. It is not recommended that you change the default value unless required by your ISP.
- **Enable NAT:** This technology translates the IP addresses of a local area network to a different IP address for the Internet. If this Modem Router is hosting your network's connection to the Internet, please select the check box. If another Router exists in your network, you don't need to select the option.
- **Enable Fullcone NAT:** It is a type of NAT, if not enabled, the default NAT will act.
- **Enable SPI Firewall:** A SPI firewall enhances network's security. Select the option to use a firewall, or else without a firewall.
- **Enable IGMP Proxy:** IGMP (Internet Group Management Protocol) is used to manage multicasting on TCP/IP networks. Some ISPs use IGMP to perform remote configuration for client devices, such as the Modem Router. The default value is disabled, and if you are not sure, please contact your ISP or just leave it.

- **Get IP Unicast:** This is disabled by default. The minority of DHCP Server of ISP will not support to enable this. When the Route is connected right but IP cannot get, you can select this box.
- **Primary DNS Server/ Secondary DNS Server:** Choose “Set DNS Server manually”, you can set DNS Server (at least one) manually here. The Route will use this DNS Server for priority.

Click the **Save** button to save the settings.

4.4.1.3 PPPoE

If your ISP provides a **PPPoE** connection and you need to use an ATM Interface, choose **PPPoE** in the drop-down list, and then the screen will be displayed as below.

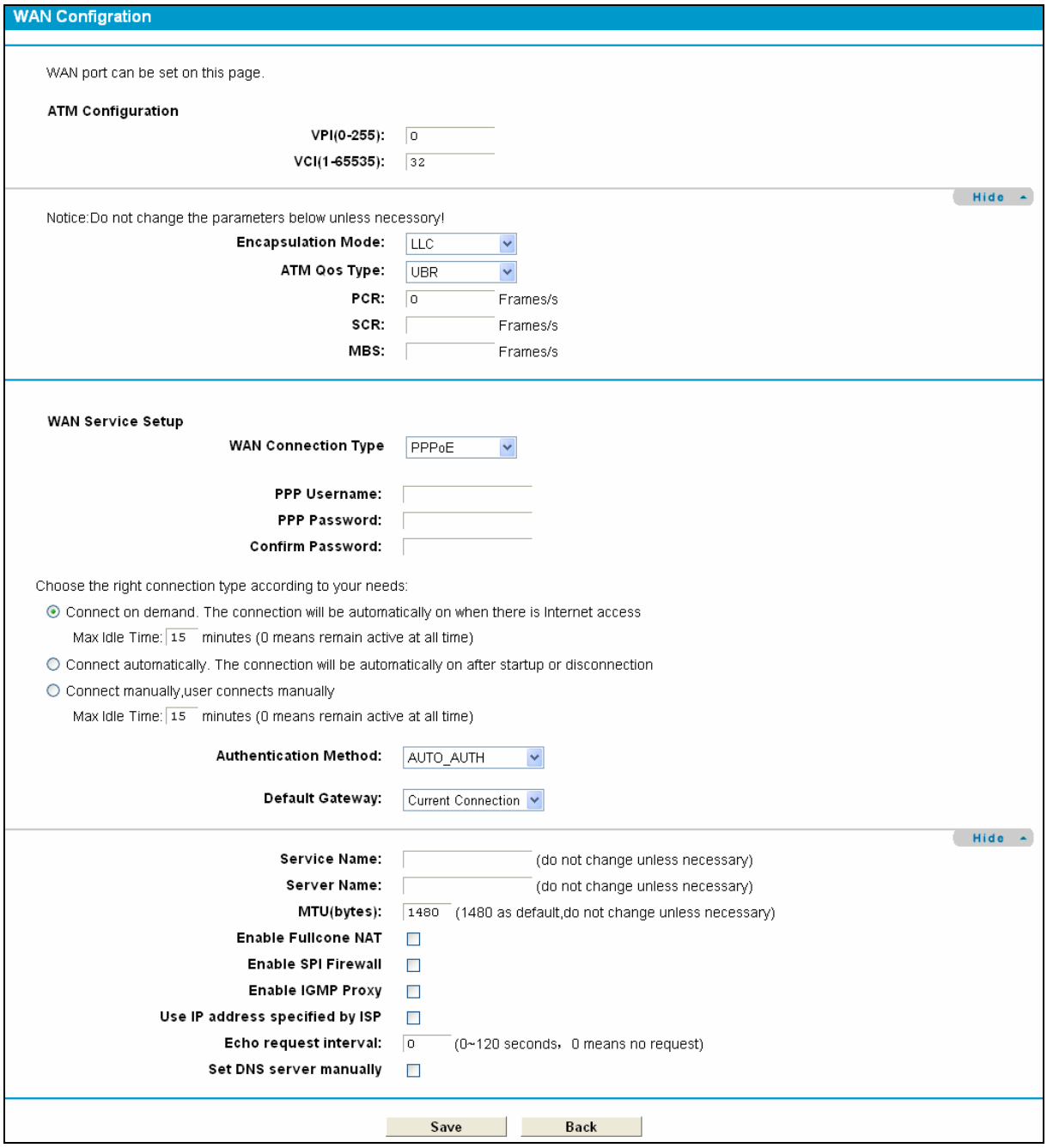

WAN Configration
WAN port can be set on this page.
ATM Configuration
VPI(0-255): 0
VCI(1-65535): 32
Hide
Notice:Do not change the parameters below unless necessary!
Encapsulation Mode: LLC
ATM Qos Type: UBR
PCR: 0 Frames/s
SCR: Frames/s
MBS: Frames/s
WAN Service Setup
WAN Connection Type PPPoE
PPP Username:
PPP Password:
Confirm Password:
Choose the right connection type according to your needs:
Connect on demand. The connection will be automatically on when there is Internet access
Max Idle Time: 15 minutes (0 means remain active at all time)
Connect automatically. The connection will be automatically on after startup or disconnection
Connect manually,user connects manually
Max Idle Time: 15 minutes (0 means remain active at all time)
Authentication Method: AUTO_AUTH
Default Gateway: Current Connection
Hide
Service Name: (do not change unless necessary)
Server Name: (do not change unless necessary)
MTU(bytes): 1480 (1480 as default,do not change unless necessary)
Enable Fullcone NAT
Enable SPI Firewall
Enable IGMP Proxy
Use IP address specified by ISP
Echo request interval: 0 (0~120 seconds，0 means no request)
Set DNS server manually
Save
Back

Figure 4-6

- **PPP Username/Password/Confirm Password:** Enter the User Name, Password and Confirm Password provided by your ISP. These fields are case-sensitive.
- **Authentication Method:** Select the **Authentication Method** from the drop-down list, the default method is **AUTO_AUTH**, and you can leave it as a default setting.
- **Choose the right connection type according to your needs:** For PPPoE connection, you can select **Connect on demand** or **Connect automatically** or **Connect manually**. Connect on demand is dependent on the traffic. If there is no traffic (or **Idle**) for a pre-specified period of time), the connection will tear down automatically. And once there is traffic send or receive, the connection will be automatically on.

Click **Advanced**, advanced selections for WAN Service Setup can be shown.

- **Service Name/Server Name:** Enter the Service Name and Server Name if it was provided by your ISP. You can leave them blank, if the ISP doesn't provide them.

4.4.1.4 PPPoA

If your ISP provides a **PPPoA** connection and you need to use an ATM Interface, choose **PPPoA** in the drop-down list, and then the screen will be displayed as below.

The configuration is similar to **PPPoE**. Please refer to the section 4.4.14 PPPoE to configure this part.

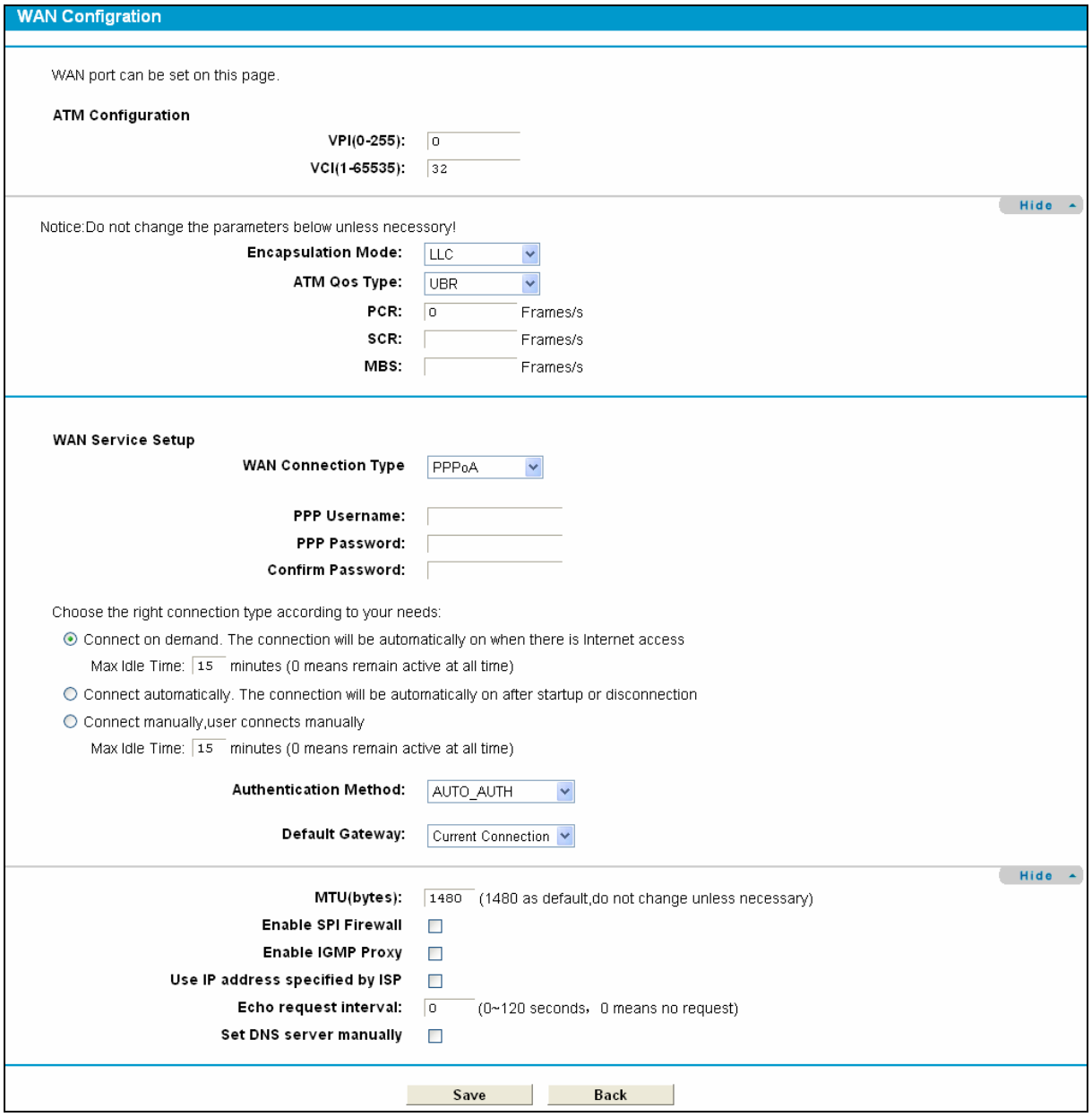

WAN Configration
WAN port can be set on this page.
ATM Configuration
VPI(0-255): 0
VCI(1-65535): 32
Hide
Notice:Do not change the parameters below unless necessory!
Encapsulation Mode: LLC
ATM Qos Type: UBR
PCR: 0 Frames/s
SCR: Frames/s
MBS: Frames/s
WAN Service Setup
WAN Connection Type PPPoA
PPP Username:
PPP Password:
Confirm Password:
Choose the right connection type according to your needs:
Connect on demand. The connection will be automatically on when there is Internet access
Max Idle Time: 15 minutes (0 means remain active at all time)
Connect automatically. The connection will be automatically on after startup or disconnection
Connect manually,user connects manually
Max Idle Time: 15 minutes (0 means remain active at all time)
Authentication Method: AUTO_AUTH
Default Gateway: Current Connection
Hide
MTU(bytes): 1480 (1480 as default,do not change unless necessary)
Enable SPI Firewall
Enable IGMP Proxy
Use IP address specified by ISP
Echo request interval: 0 (0~120 seconds，0 means no request)
Set DNS server manually
Save
Back

Figure 4-7

4.4.1.5 IPoA

If your ISP provides an IPoA connection, select **IPoA** option for the **WAN service type** on the screen.

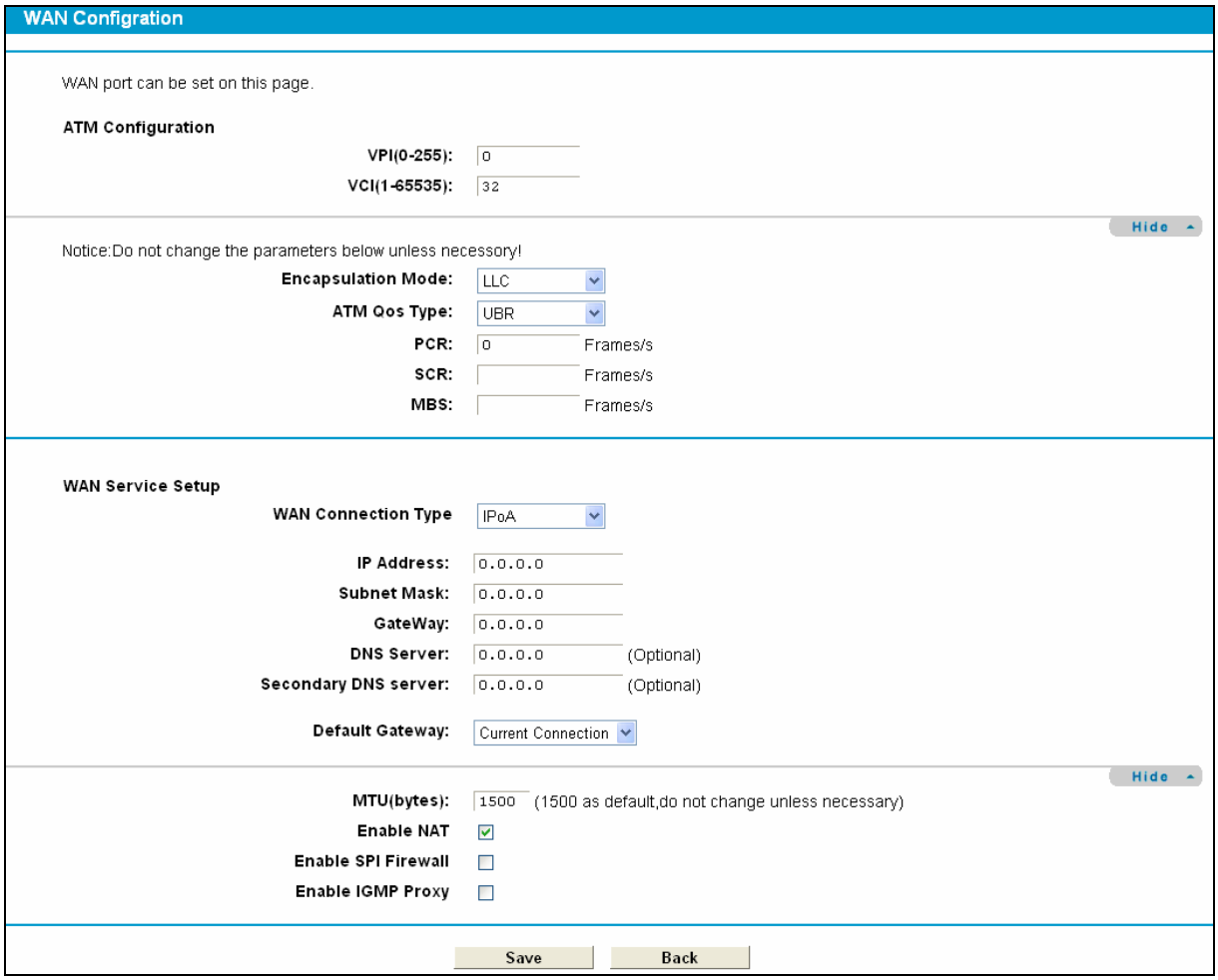


Figure 4-8

- **IP Address/Subnet Mask:** Enter the IP Address and Subnet Mask provided by ISP. If you forget, you can ask your ISP.
- **DNS Server/Secondary DNS Server:** Type in your preferred DNS server.
- **Default Gateway:** select a WAN Interface from the drop-down list as the IPv4 default gateway.

4.4.1.6 Bridge

If you select this type of connection, the modem can be configured to act as a bridging device between your LAN and your ISP. Bridges are devices that enable two or more networks to communicate as if they are two segments of the same physical LAN.

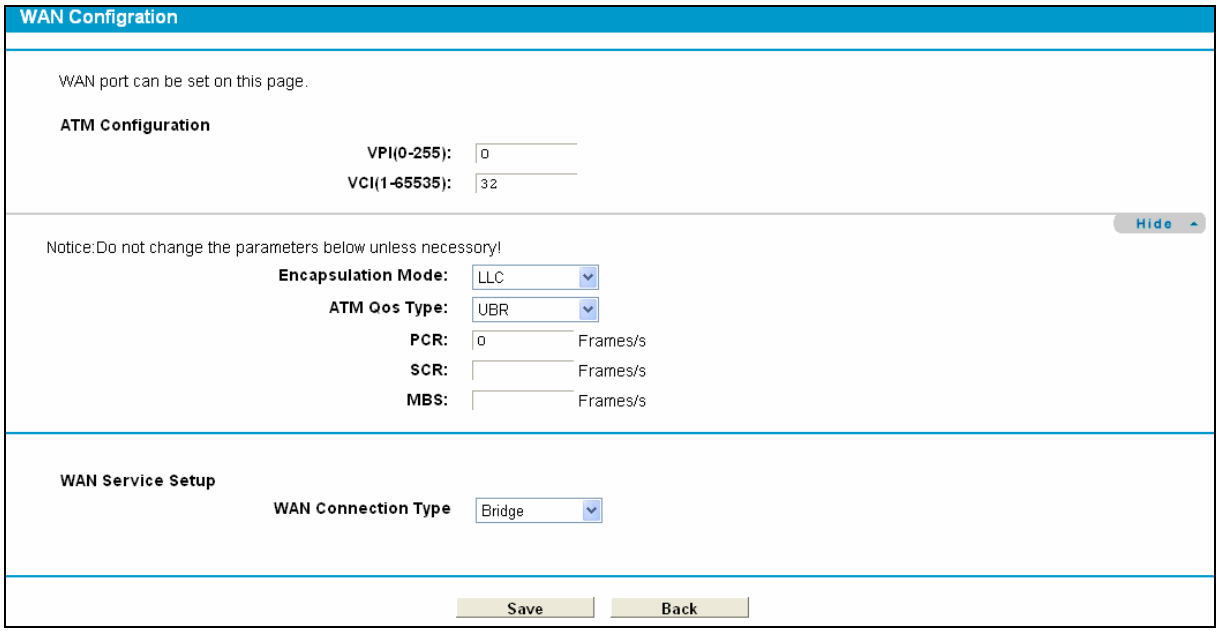


Figure 4-9

Note:

After you finish the Internet configuration, please click **Save** to make the settings take effect.

4.4.2 EWAN

Choose "**Network**"→"**EWAN**", and you will see the Ethernet WAN Interface screen similar to Figure 4-10. There are there different configurations for the connection types, which are Dynamic IP, Static IP and PPPoE. You can select the corresponding types according to your needs.

Note:

1) EWAN and DSL interface can not be used concurrently. If the EWAN Interface had configured, you cannot configure any other WAN service over the DSL Interface until the EWAN Interface is deleted.
2) If EWAN function is be enabled, LAN4/WAN port of the Modem Router changes to be WAN port which can be connected to the cable, VDSL or Fiber modem.

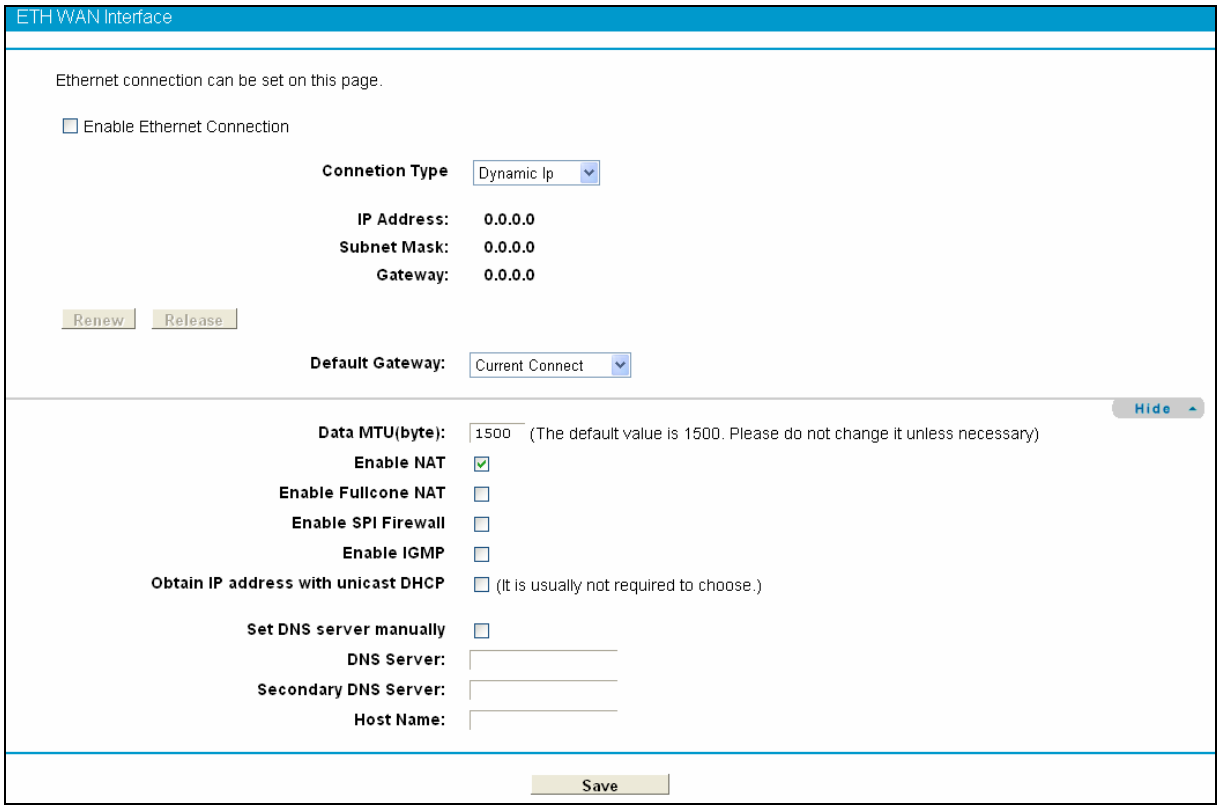


Figure 4-10

4.4.2.1 Dynamic IP

Select this option, the Modem Router will be able to obtain IP network information dynamically from a DHCP server provided by your ISP (as shown Figure 4-10). The next configuration is similar to **Dynamic IP** over ATM interface (see section 4.4.1.2 Dynamic IP)

4.4.2.2 Static IP

Select this option if your ISP provides static IP information to you and you want to use an **Ethernet** Interface. You should set static IP address, IP subnet mask, gateway address, DNS Server and Secondary DNS Server in the screen below. The next configuration is similar to **Static IP** for WAN Settings (see section 4.4.1.1 Static IP)

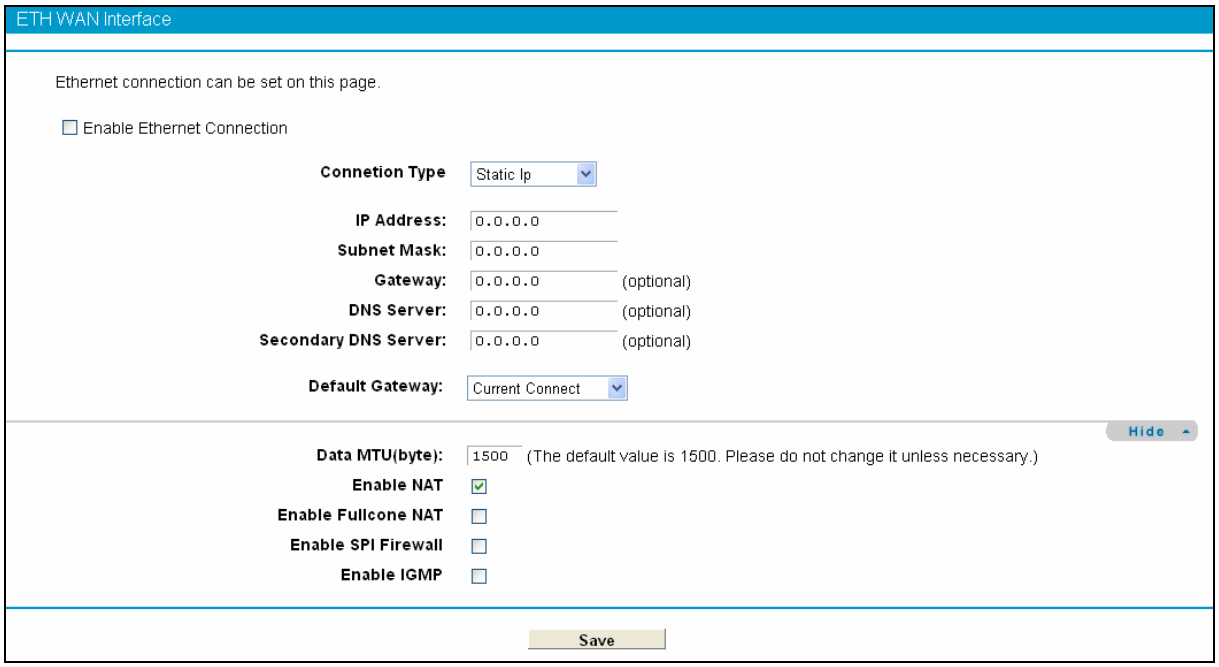


Figure 4-11

4.4.2.3 PPPoE

If your ISP provides a **PPPoE** connection and you need to use an **Ethernet** Interface, select **PPPoE** option for the **WAN service type** on the screen. The following configuration is similar to **PPPoE** over ATM interface (see section 4.4.1.3 PPPoE).

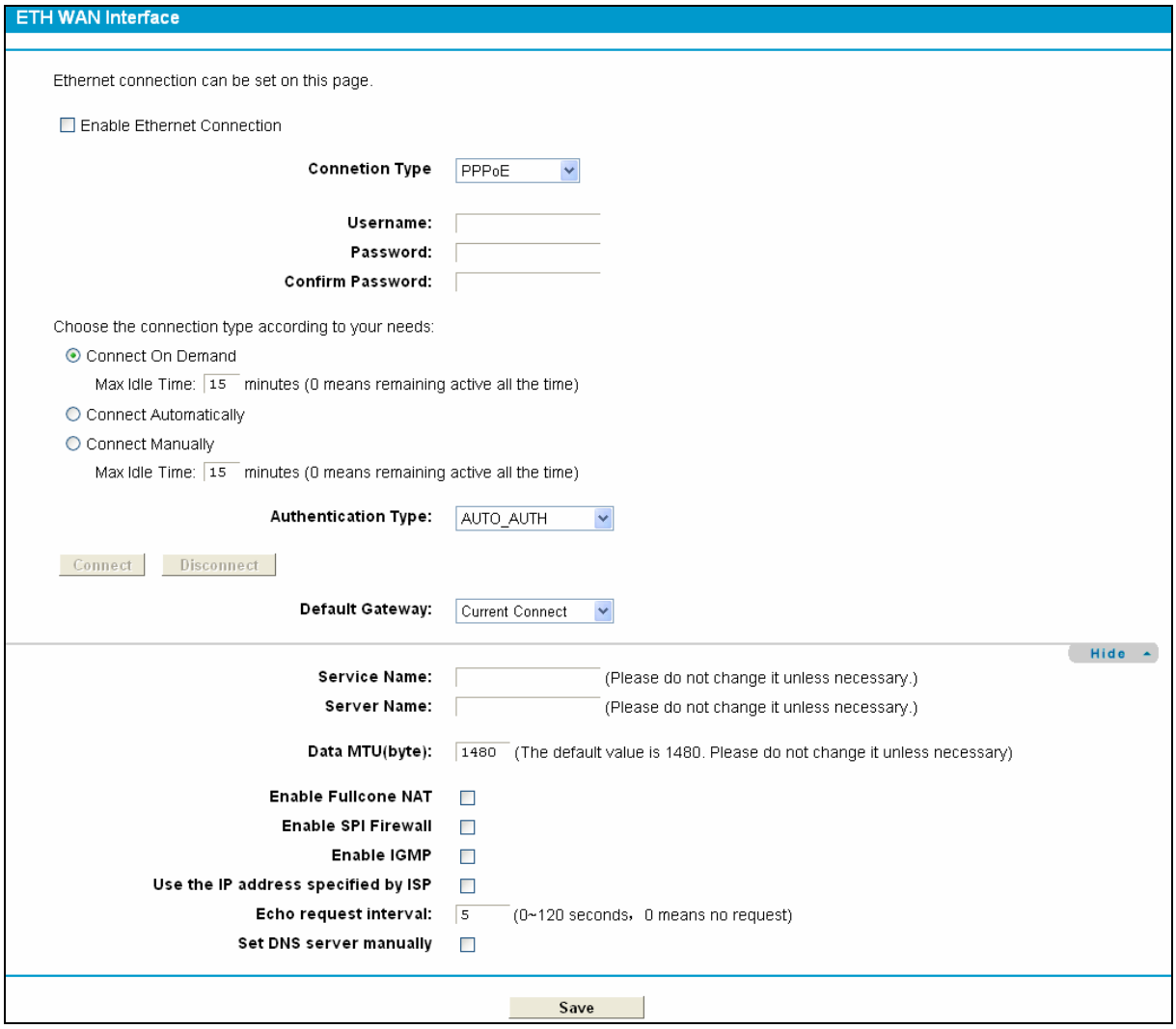


Figure 4-12

4.4.3 Interface Grouping

Choose "**Network**"→"**Interface Grouping**", you can view all the current groups on this page (shown in Figure 4-13).

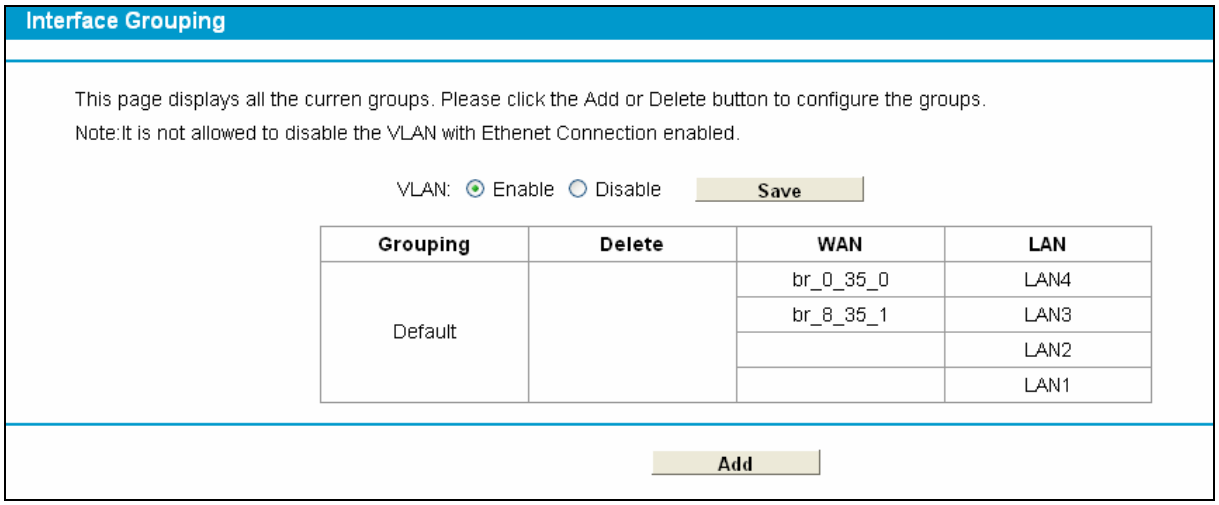


Figure 4-13

- **VLAN:** Enable or disable this function. Virtual LAN (VLAN) is a group of devices on one or more LANs that are configured so that they can communicate as if they were attached to the same LAN, when in fact they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, it is very flexible for user/host management, bandwidth allocation and resource optimization. If you want to active this function, this function must be enabled.

☞ **Note:**

It is not allowed to disable the VLAN with Ethernet Connection enabled.

To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the **Add** button. The **Remove** button will remove the grouping and add the ungrouped interfaces to the Default group. Only the default group has IP interface.

Click the **Add** button. You can add a new interface group in the next screen. For example, you want LAN1 and LAN3 to be a group called Group 1 over br_0_35_0 WAN interface, you can refer to the following figure.

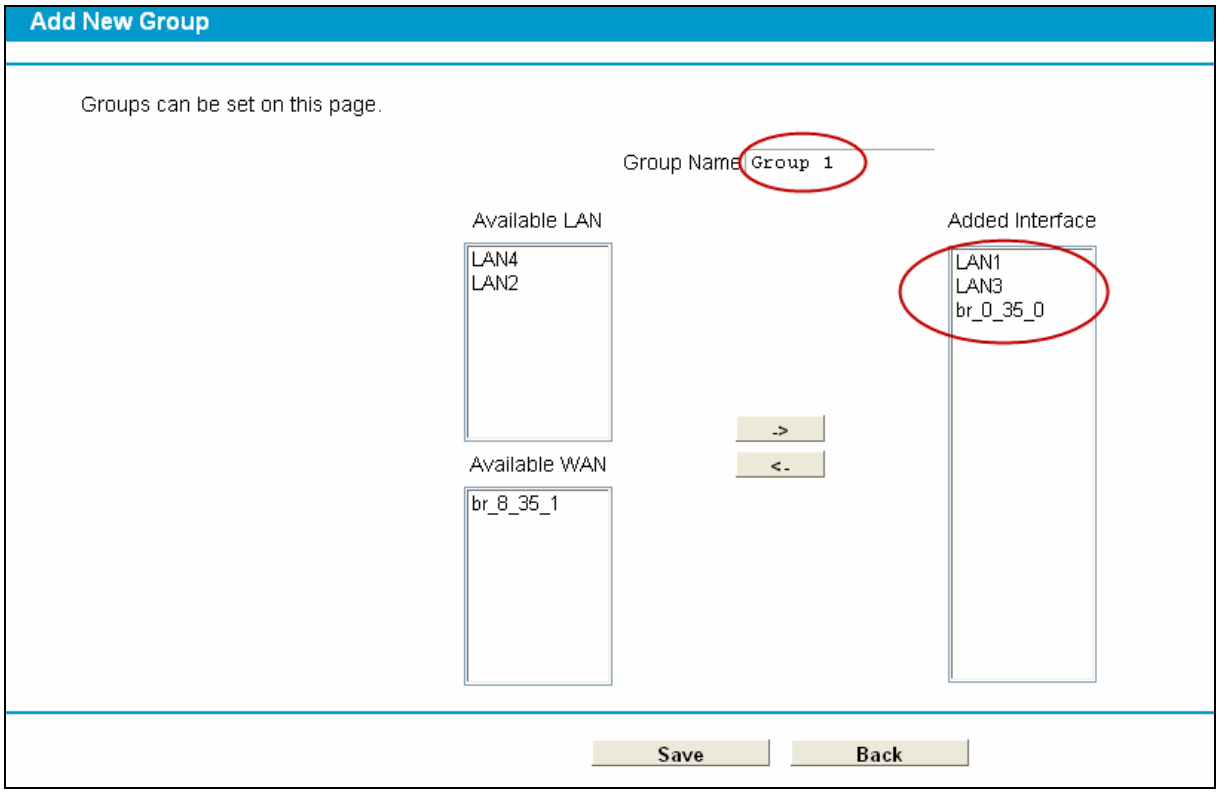


Figure 4-14

Click **Save** to make the entry effective immediately

4.4.4 LAN Settings

Choose "**Network**"→"**LAN Settings**" menu, and you will see the LAN screen (shown in Figure 4-15). Please configure the parameters for LAN ports according to the descriptions below.

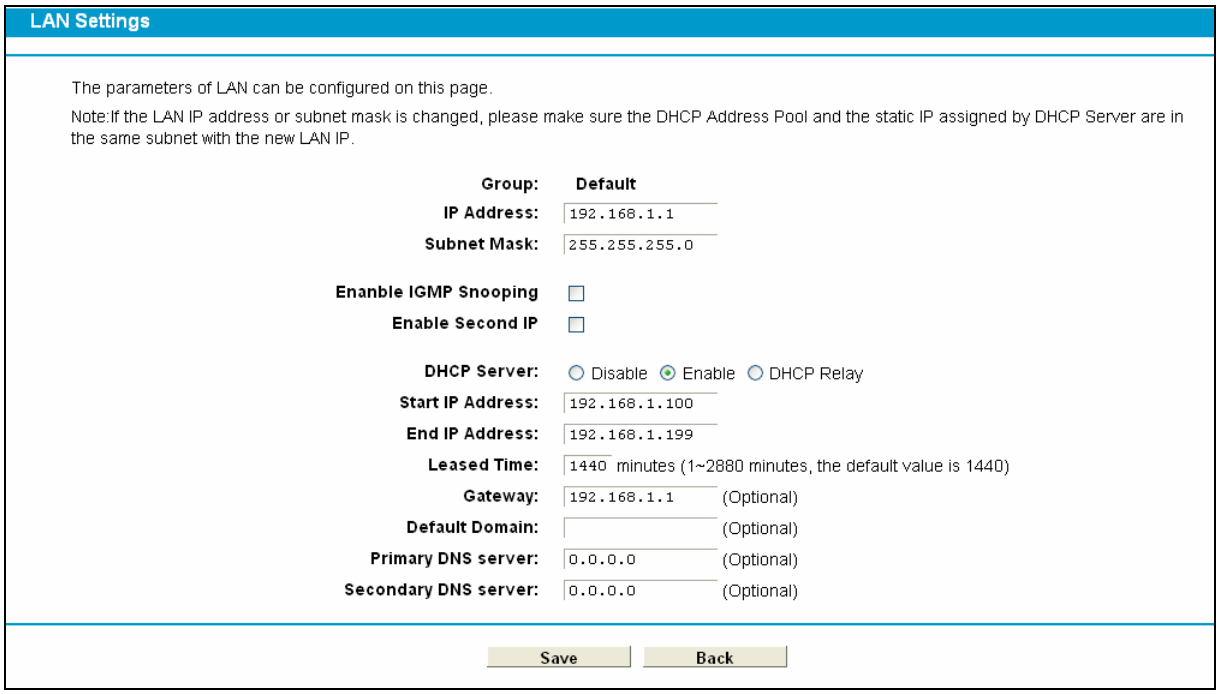

LAN Settings
The parameters of LAN can be configured on this page.
Note:If the LAN IP address or subnet mask is changed, please make sure the DHCP Address Pool and the static IP assigned by DHCP Server are in the same subnet with the new LAN IP.
Group: Default
IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0
Enanble IGMP Snooping
Enable Second IP
DHCP Server: Disable Enable DHCP Relay
Start IP Address: 192.168.1.100
End IP Address: 192.168.1.199
Leased Time: 1440 minutes (1~2880 minutes, the default value is 1440)
Gateway: 192.168.1.1 (Optional)
Default Domain: (Optional)
Primary DNS server: 0.0.0.0 (Optional)
Secondary DNS server: 0.0.0.0 (Optional)
Save
Back

Figure 4-15

- **IP Address:** You can configure the Modem Router's IP Address and Subnet Mask for LAN Interface.
  - **IP Address:** Enter the Modem Router's local IP Address, then you can access to the Web-based Utility via the IP Address, the default value is 192.168.1.1.
  - **Subnet Mask:** Enter the Modem Router's Subnet Mask, the default value is 255.255.255.0.
- **Enable IGMP Snooping:** If you select the option, please choose the IGMP Mode**:** Standard Mode or Blocking Mode.
- **Enable Second IP:** You can configure the Modem Router's second IP Address and Subnet Mask for LAN Interface through which you can also access to the Web-based Utility as the default IP Address and Subnet Mask.
- **DHCP Server:** These settings allow you to configure the Modem Router's Dynamic Host Configuration Protocol (DHCP) server function. The DHCP server is enabled by default for the Modem Router's Ethernet LAN interface. DHCP service will supply IP settings to computers which are configured to automatically obtain IP settings that are connected to the Modem Router though the Ethernet port. When the Modem Router is set for DHCP, it becomes the default gateway for DHCP client connected to it. Keep in mind that if you change the IP address of the Modem Router, you must change the range of IP addresses in the pool used for DHCP on the LAN.
  - **Start IP Address:** Enter a value for the DHCP server to start with when issuing IP addresses. Because the default IP address for the Modem Router is 192.168.1.1, the default Start IP Address is **192.168.1.100**, and the Start IP Address must be 192.168.1.100 or greater, but smaller than 192.168.1.254.
  - **End IP Address:** Enter a value for the DHCP server to end with when issuing IP addresses. The End IP Address must be smaller than 192.168.1.254. The default End IP Address is **192.168.1.254**.

- **Leased Time:** The Leased Time is the amount of time in which a network user will be allowed connection to the Modem Router with their current dynamic IP address. Enter the amount of time, in hours, then the user will be "leased" this dynamic IP address. After the dynamic IP address has expired, the user will be automatically assigned a new dynamic IP address. The default is **1440** minutes.

The detailed configuration about DHCP server, please refer to section 4.5 DHCP Server.

4.4.5 MAC Clone

Choose menu "**Advanced Setup**"→"**MAC Clone**", you can configure the MAC address of the WAN Interface as shown below.

The WAN Interface List displays the Lay2 Interfaces you have configured on the section 4.4.1 WAN Settings, 4.4.2 Ethernet WAN and its default MAC Address. You can select corresponding WAN Interface from the drop-down list and click **Clone** button to clone your current PC MAC, and then click **Save**.

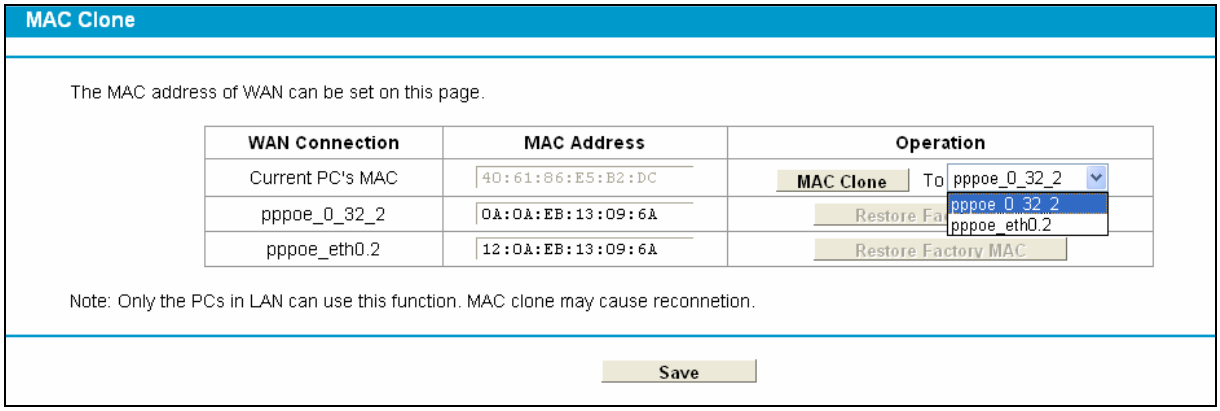


Figure 4-16

☞ **Note:**

Only the WAN Ports can use MAC Address Clone function. All the clone MAC addresses must not be the same with each other.

4.4.6 ALG Settings

Choose menu "**Advanced Setup**"→"**ALG Settings**", and then you can configure the basic security in the screen as shown in Figure 4-17.

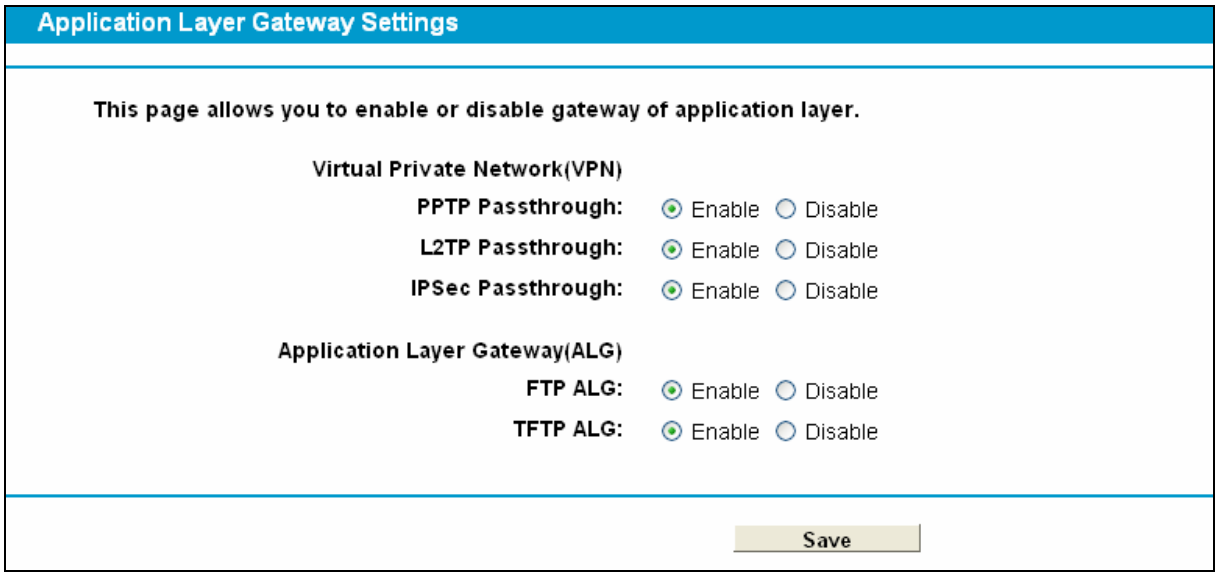

Application Layer Gateway Settings
This page allows you to enable or disable gateway of application layer.
Virtual Private Network(VPN)
PPTP Passthrough: Enable Disable
L2TP Passthrough: Enable Disable
IPSec Passthrough: Enable Disable
Application Layer Gateway(ALG)
FTP ALG: Enable Disable
TFTP ALG: Enable Disable
Save

Figure 4-17

- **Virtual Private Network (VPN) -** VPN Passthrough must be enabled if you want to allow VPN tunnels using VPN protocols to pass through the Modem Router.

  - **PPTP Passthrough** - Point-to-Point Tunneling Protocol (PPTP) allows the Point-to-Point Protocol (PPP) to be tunneled through an IP network. To allow PPTP tunnels to pass through the Modem Router, click **Enable**.
  - **L2TP Passthrough** - Layer Two Tunneling Protocol (L2TP) is the method used to enable Point-to-Point sessions via the Internet on the Layer Two level. To allow L2TP tunnels to pass through the Modem Router, click **Enable**.
  - **IPSec Passthrough** - Internet Protocol security (IPSec) is a suite of protocols for ensuring private, secure communications over Internet Protocol (IP) networks, through the use of cryptographic security services. To allow IPSec tunnels to pass through the Modem Router, click **Enable**.

- **Application Layer Gateway (ALG) -** It is recommended to enable Application Layer Gateway (ALG) because ALG allows customized Network Address Translation (NAT) traversal filters to be plugged into the gateway to support address and port translation for certain application layer "control/data" protocols such as FTP, TFTP etc.

  - **FTP ALG** - To allow FTP clients and servers to transfer data across NAT, click **Enable**.
  - **TFTP ALG** - To allow TFTP clients and servers to transfer data across NAT, click **Enable**.

Click the **Save** button to save your settings.

4.4.7 DSL Settings

Choose "**Advanced Setup**"→"**DSL Settings**", you can select the DSL Modulation Type and Annex Type in the next screen. The DSL feature can be selected when you meet the physical connection problem. Please check the proper settings with your Internet service provider.

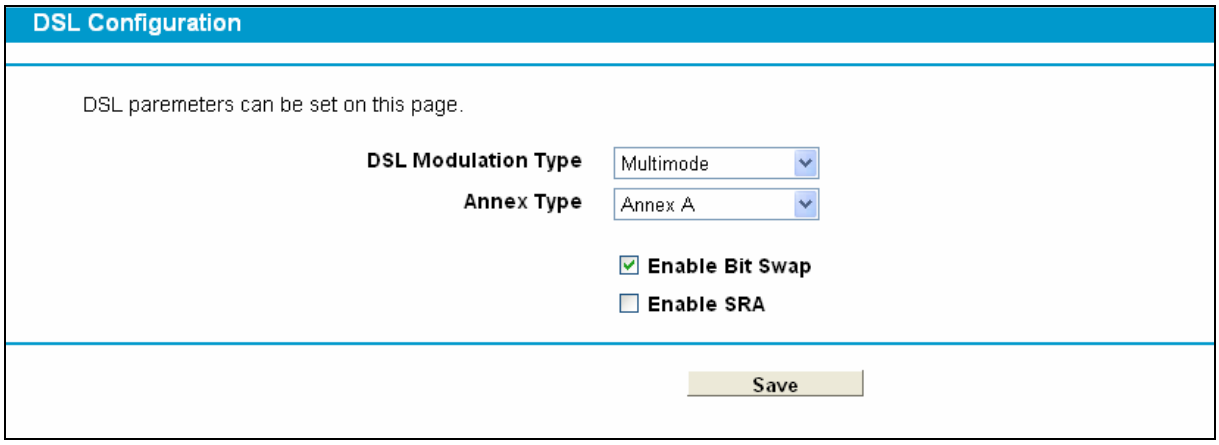


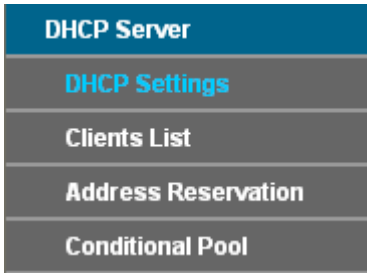
Figure 4-18

- **DSL Modulation Type:** Select the DSL operation Modulation Type which your DSL connection uses.
- **Annex Type:** Select the DSL operation Annex Type which your DSL connection uses.

Click the **Save** button to save your settings.

4.5 DHCP Server

Choose "**DHCP Server**", you can see the next submenus:



Click any of them, and you will be able to configure the corresponding function.

4.5.1 DHCP Settings

Choose menu "**DHCP Server**"→"**DHCP Settings**", you can configure the DHCP Server on the page as shown in Figure 4-19.The Modem Router is set up by default as a DHCP (Dynamic Host Configuration Protocol) server, which provides the TCP/IP configuration for all the PC(s) that are connected to the Modem Router on the LAN.

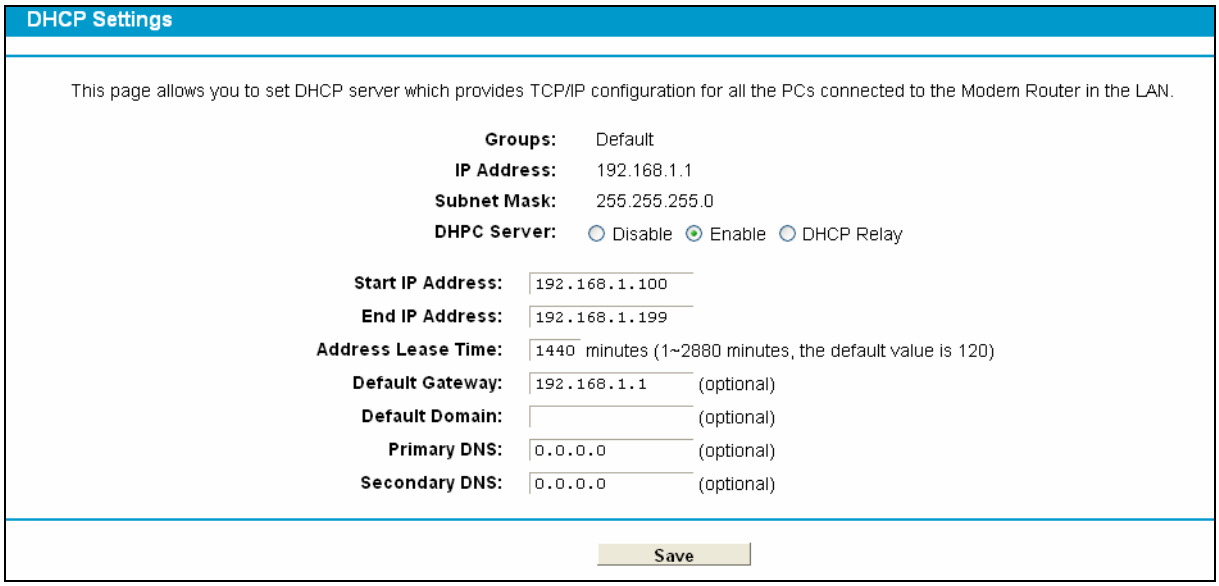
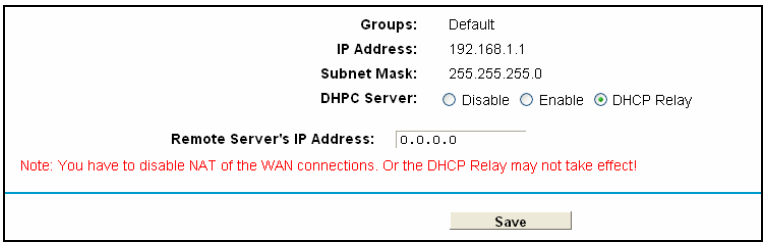

DHCP Settings
This page allows you to set DHCP server which provides TCP/IP configuration for all the PCs connected to the Modem Router in the LAN.
Groups: Default
IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0
DHPC Server: Disable Enable DHCP Relay
Start IP Address: 192.168.1.100
End IP Address: 192.168.1.199
Address Lease Time: 1440 minutes (1~2880 minutes, the default value is 120)
Default Gateway: 192.168.1.1 (optional)
Default Domain: (optional)
Primary DNS: 0.0.0.0 (optional)
Secondary DNS: 0.0.0.0 (optional)
Save

Figure 4-19

- **Start IP Address:** Enter a value for the DHCP server to start with when issuing IP addresses. Because the default IP address for the Modem Router is 192.168.1.1, the default Start IP Address is **192.168.1.100**, and the Start IP Address must be 192.168.1.100 or greater, but smaller than 192.168.1.254.
- **End IP Address:** Enter a value for the DHCP server to end with when issuing IP addresses. The End IP Address must be smaller than 192.168.1.254. The default End IP Address is **192.168.1.254**.
- **Address Lease Time:** The Leased Time is the amount of time in which a network user will be allowed connection to the Modem Router with their current dynamic IP address. Enter the amount of time, in hours, then the user will be "leased" this dynamic IP address. After the dynamic IP address has expired, the user will be automatically assigned a new dynamic IP address. The default is **24** hours.
- **Default Gateway - (Optional):** It is suggested to input the IP address of the LAN port of the Modem Router. The default value is 192.168.1.1.
- **Default Domain - (Optional):** Input the domain name of your network.
- **Primary DNS - (Optional):** Input the DNS IP address provided by your ISP or consult your ISP.
- **Secondary DNS - (Optional):** Input the IP address of another DNS server if your ISP provides two DNS servers.
- **DHCP Relay:** Select **Relay**, then you will see the next screen, and the Modem Router will work as a DHCP Relay. A DHCP relay is a computer that forwards DHCP data between computers that request IP addresses and the DHCP server that assigns the addresses. Each of the device's interfaces can be configured as a DHCP relay. If it is enabled, the DHCP requests from local PCs will forward to the DHCP server runs on WAN side. To have this function working properly, please run on router mode only, disable the DHCP server on the LAN port, and make sure the routing table has the correct routing entry.


Groups: Default
IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0
DHPC Server: Disable Enable DHCP Relay
Remote Server's IP Address: 0.0.0.0
Note: You have to disable NAT of the WAN connections. Or the DHCP Relay may not take effect!
Save

Note:

1) To use the DHCP server function of the Modem Router, you must configure all computers on the LAN as "Obtain an IP Address automatically".
2) You have to disable NAT of the WAN connections, or the DHCP Relay may not take effect.
3) If you select **Disabled**, the DHCP function will not take effect.

Click the **Save** button to save your settings.

4.5.2 Clients List

Choose menu "**DHCP Server**"→"**Clients List**", you can view the information about the clients attached to the Modem Router in the screen as shown in Figure 4-20.

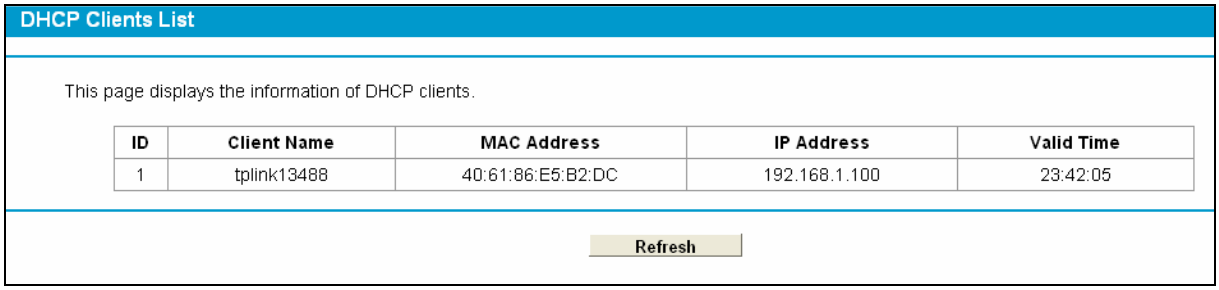


Figure 4-20

- **Client Name:** The name of the DHCP client
- **MAC Address:** The MAC address of the DHCP client
- **IP Address:** The IP address that the Modem Router has allocated to the DHCP client
- **Valid Time:** The time of the DHCP client leased. After the dynamic IP address has expired, a new dynamic IP address will be automatically assigned to the user.

You cannot change any of the values on this page. To update this page and to show the current attached devices, click the **Refresh** button.

4.5.3 Address Reservation

Choose menu "**DHCP Server**"→"**Address Reservation**", you can view and add a reserved address for clients via the next screen (shown in Figure 4-21).When you specify a reserved IP address for a PC on the LAN, that PC will always receive the same IP address each time when it accesses the DHCP server. Reserved IP addresses should be assigned to the servers that require permanent IP settings.

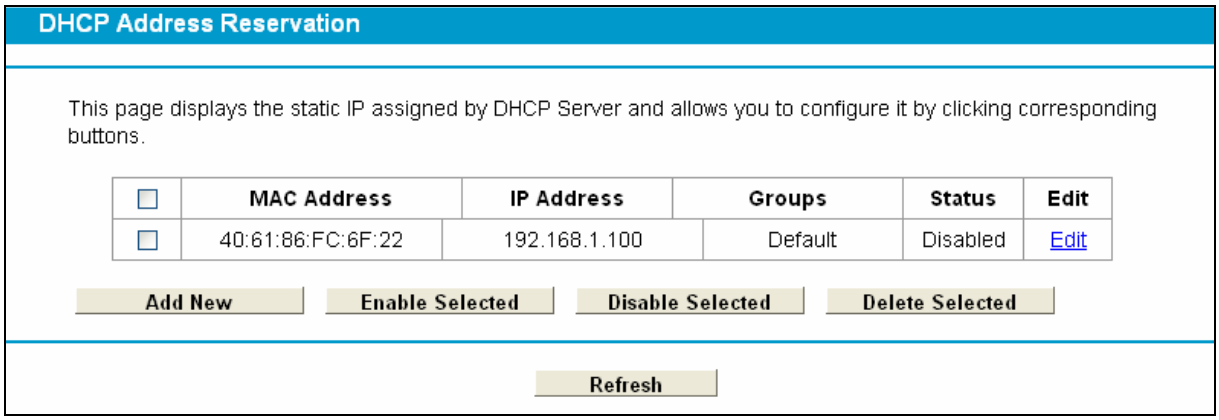


Figure 4-21

- **MAC Address:** The MAC address of the PC for which you want to reserve an IP address.
- **IP Address:** The IP address reserved for the PC by the Modem Router.
- **Status:** The status of this entry either **Enabled** or **Disabled**.

To Reserve an IP address:

1. Click the **Add New** button. Then Figure 4-22 will pop up.
2. Enter the MAC address (in XX:XX:XX:XX:XX:XX format.) and IP address (in dotted-decimal notation) of the computer for which you want to reserve an IP address.
3. Click the **Save** button.

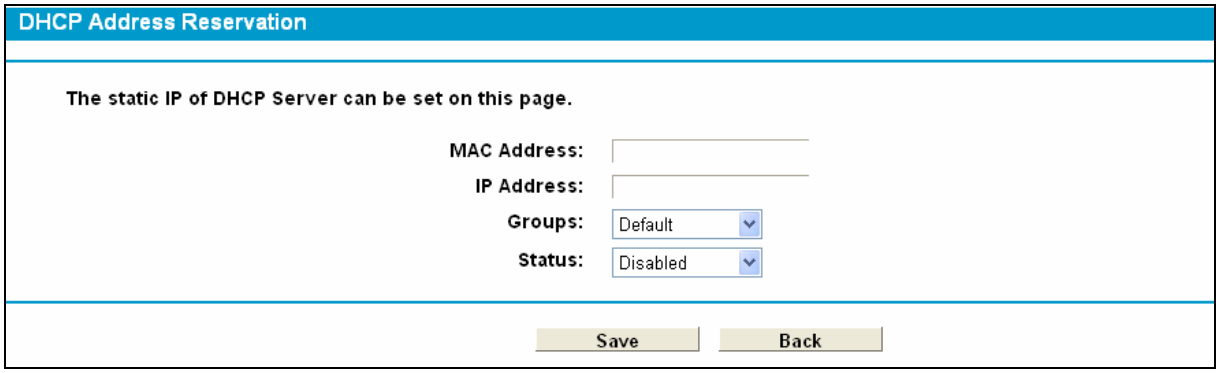


Figure 4-22

To modify or delete an existing entry:

1. Click the **Edit** in the entry you want to modify. If you want to delete the entry, click the **Delete**.
2. Modify the information.
3. Click the **Save** button.

Click the **Enable/Disable Selected** button to make selected entries enabled/disabled.

Click the **Delete Selected** button to selected entries.

4.5.4 Conditional Pool

Choose menu "**DHCP Server**"→"**Conditional Pool**", you can see the next screen (shown in Figure 4-23). This page displays vendor class settings and allows you to set parameters for vendor class by clicking corresponding buttons.

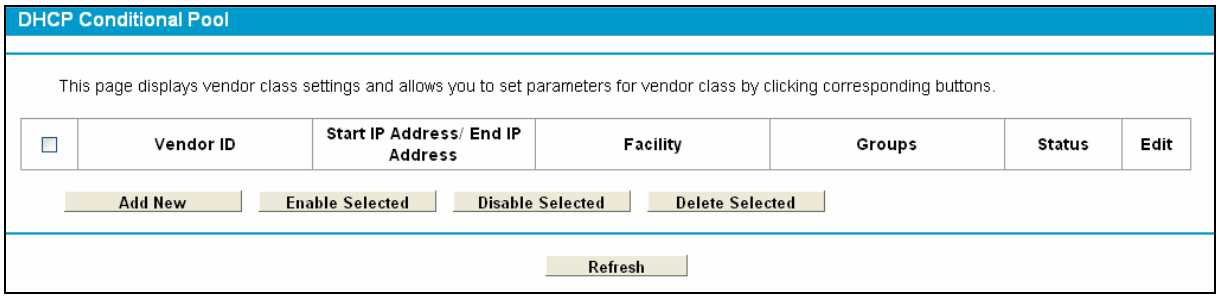


Figure 4-23

To add a vendor class:

1. Click the **Add New** button. Then Figure 4-24 will pop up.
2. Enter parameters for the vendor class.

Click the **Save** button.

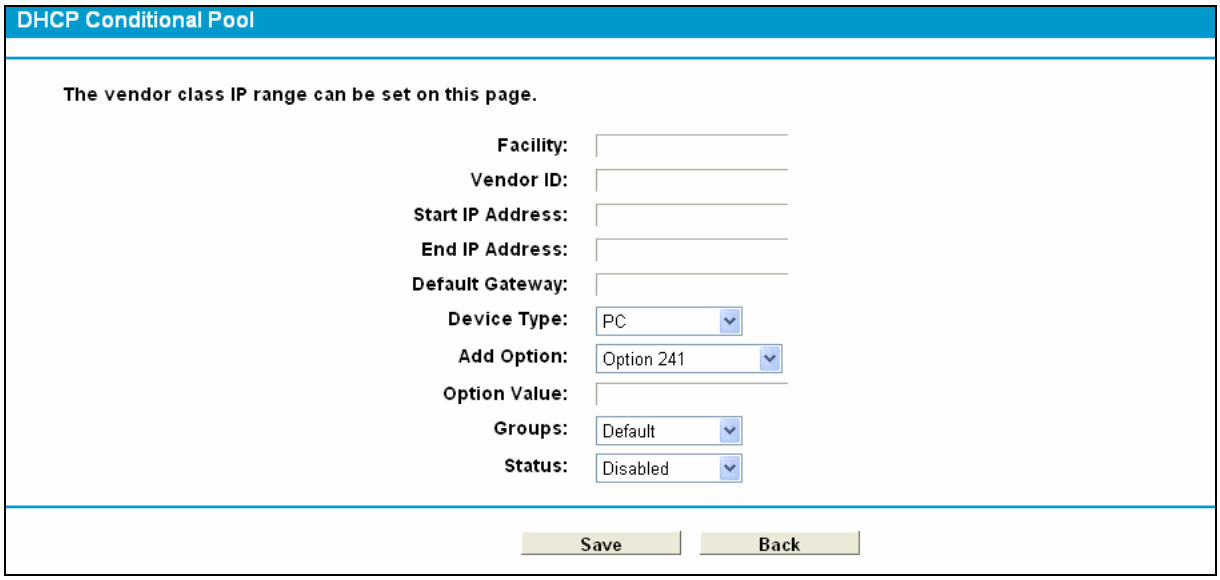


Figure 4-24

To modify or delete an existing entry:

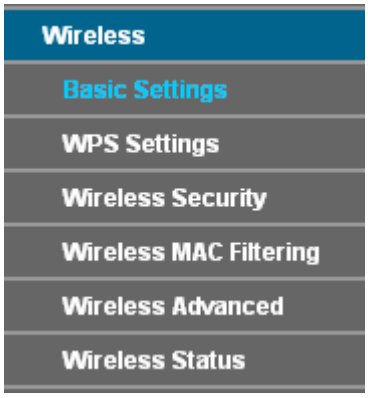
4. Click the **Edit** in the entry you want to modify. If you want to delete the entry, click the **Delete**.
5. Modify the information.
6. Click the **Save** button.

Click the **Enable/Disable Selected** button to make selected entries enabled/disabled.

Click the **Delete Selected** button to selected entries.

4.6 Wireless

Choose "**Wireless**", there are six submenus to configure Wireless LAN settings. Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.



4.6.1 Basic Settings

Choose "**Wireless**"→"**Basic**", you will see the screen of **Wireless--Basic** settings shown as below. The basic settings for wireless networking are set on this screen.

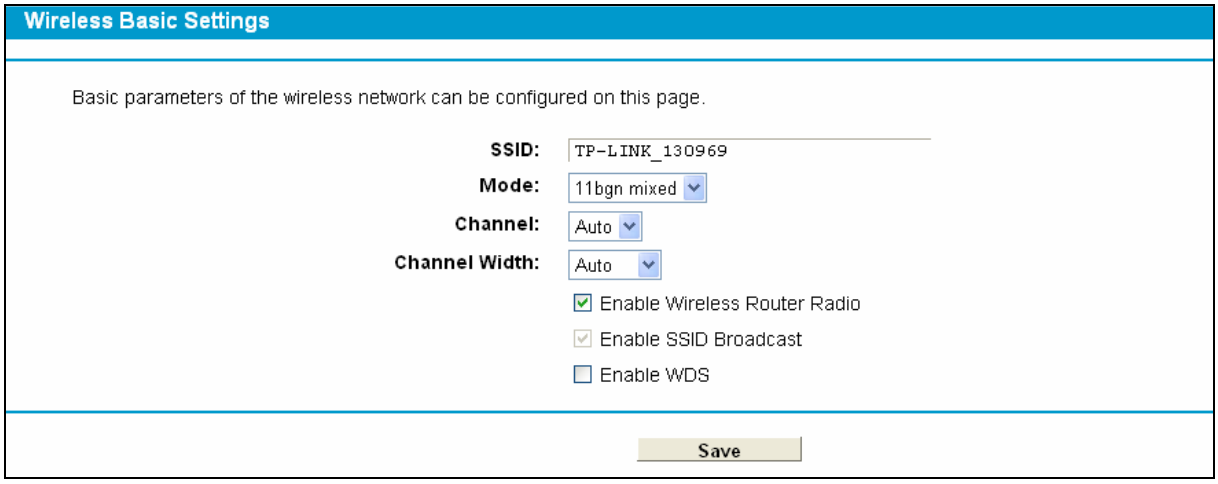


Figure 4-25

This page allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the channel set based on Region requirements.

- **SSID:** Wireless network name shared among all points in a wireless network. The SSID must be identical for all devices in the wireless network. It is case-sensitive and must not exceed 32 characters (use any of the characters on the keyboard). Make sure this setting is the same for all stations in your wireless network. Type the desired SSID in the space provided.
- **Mode:** Select the desired mode.

  11b only: Select if all of your wireless clients are 802.11b.

  11g only: Select if all of your wireless clients are 802.11g.

  11n only: Select only if all of your wireless clients are 802.11n.

11bg mixed: Select if you are using both 802.11b and 802.11g wireless clients.

11bgn mixed: Select if you are using a mix of 802.11b, 11g, and 11n wireless clients.

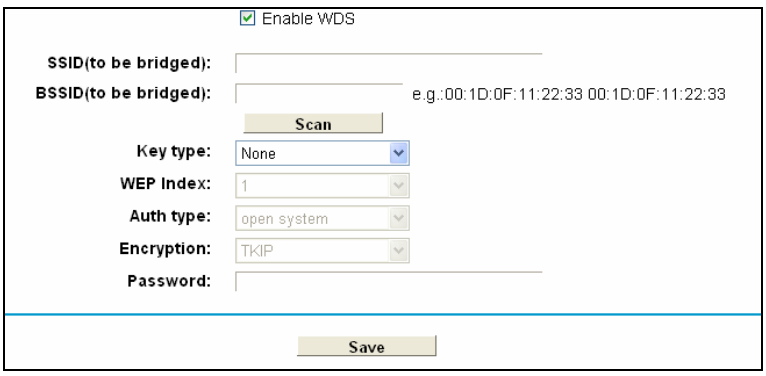
Select the desired wireless mode. When 802.11g mode is selected, only 802.11g wireless stations can be connected to the Modem Router. When 802.11n mode is selected, only 802.11n wireless stations can connect to the Modem Router. It is strongly recommended that you set the Mode to **802.11b&g&n**, and all of 802.11b, 802.11g, and 802.11n wireless stations can connect to the Modem Router.

- **Channel:** Select the channel you want to use from the drop-down List of Channel. This field determines which operating frequency will be used. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point.
- **Channel Width:** Select the channel width from the drop-down list. The default setting is automatic, which can adjust the channel width for your clients automatically.

☞ **Note:**

If **11b only**, **11g only**, or **11bg mixed** is selected in the **Mode** field, the **Channel Width** selecting field will turn grey and the value will become 20M, which is unable to be changed.

- **Enable Wireless Router Radio:** If you want to use wireless features, you must select “Enable Wireless Router Radio”. If you deselect “Enable Wireless Router Radio” option, all the Wireless settings below will be disabled.
- **Enable SSID Broadcast:** When wireless clients survey the local area for wireless networks to associate with, they will detect the SSID broadcast by the Modem Router. If you select the **Enable SSID Broadcast** checkbox, the Wireless Router will broadcast its name (SSID) on the air.
- **Enable WDS:** Check this box to enable WDS. With this function, the Modem Router can bridge two or more Wlans. If this checkbox is selected, you will have to set the following parameters as shown in the figure below. Make sure the following settings are correct.



- **SSID (to be bridged):** The SSID of the AP your Modem Router is going to connect to as a client. You can also use the search function to select the SSID to join.
- **BSSID (to be bridged):** The BSSID of the AP your Modem Router is going to connect to as a client. You can also use the search function to select the BSSID to join.
- **Scan:** Click this button, you can search the AP which runs in the current channel.
- **Key type**: This option should be chosen according to the AP's security configuration. It is recommended that the security type is the same as your AP's security type

- **WEP Index:** This option should be chosen if the key type is WEP(ASCII) or WEP(HEX). It indicates the index of the WEP key.
- **Auth Type:** This option should be chosen if the key type is WEP(ASCII) or WEP(HEX). It indicates the authorization type of the Root AP.
- **Password:** If the AP your Modem Router is going to connect needs password, you need to fill the password in this blank.

Click **Save** to save your settings.

4.6.2 WPS Settings

This section will guide you to add a new wireless device to an existing network quickly by **WPS** (also called **QSS**) function.

a). Choose menu "**WPS Settings**", and you will see the next screen (shown in Figure 4-26).

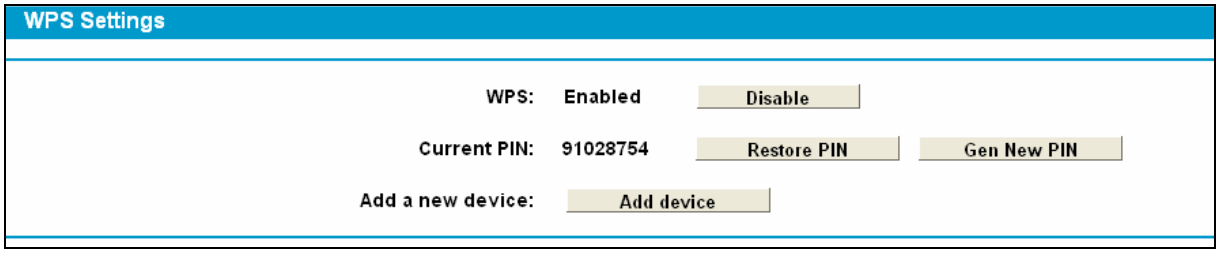


Figure 4-26

- **WPS:** Enable or disable the WPS function here.
- **Current PIN:** The current value of the Modem Router's PIN is displayed here. The default PIN of the Modem Router can be found in the label or User Guide.
- **Restore PIN:** Restore the PIN of the Modem Router to its default.
- **Gen New PIN:** Click this button, and then you can get a new random value for the Modem Router's PIN. You can ensure the network security by generating a new PIN.
- **Add device:** You can add a new device to the existing network manually by clicking this button.

b). To add a new device:

If the wireless adapter supports Wi-Fi Protected Setup (WPS), you can establish a wireless connection between wireless adapter and Modem Router using either Push Button Configuration (PBC) method or PIN method.

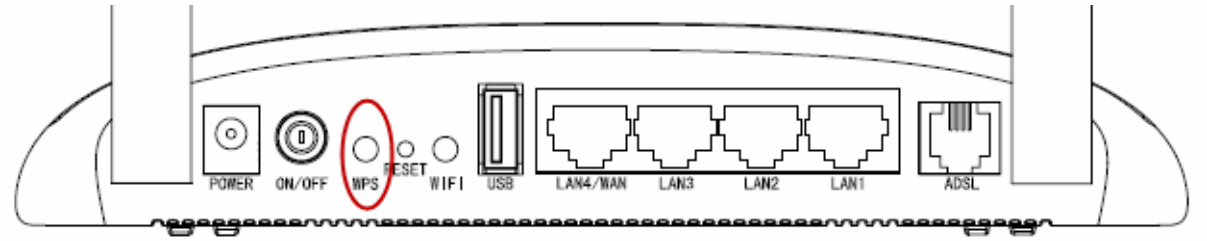
☞ **Note:**

To build a successful connection by WPS, you should also do the corresponding configuration of the new device for WPS function meanwhile.

I. Use the Wi-Fi Protected Setup Button

Use this method if your client device has a Wi-Fi Protected Setup button.

Step 1: Press the WPS button on the back panel of the Modem Router, as shown in the following figure.



You can also keep the default WPS Status as **Enabled** and click the **Add device** button in Figure 4-26, then Choose "**Press the button of the new device in two minutes**" and click **Connect**. (Shown in the following figure)

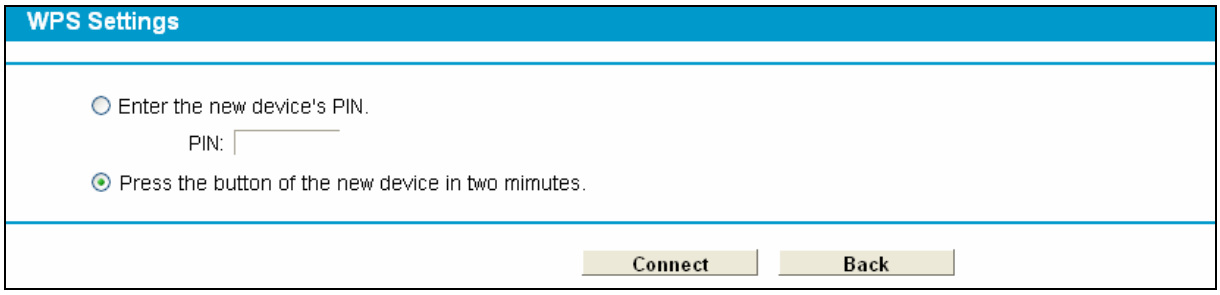


Figure 4-27

Step 2: Press and hold the WPS button of the client device directly.

Step 3: The Wi-Fi Protected Setup LED flashes for two minutes during the Wi-Fi Protected Setup process.

Step 4: When the WPS LED is on, the client device has successfully connected to the Modem Router.

Refer back to your client device or its documentation for further instructions.

II. Enter the client device's PIN on the Modem Router

Use this method if your client device has a Wi-Fi Protected Setup PIN number.

Step 1: Keep the default WPS Status as **Enabled** and click the **Add device** button in Figure 4-26, then the following screen will appear.

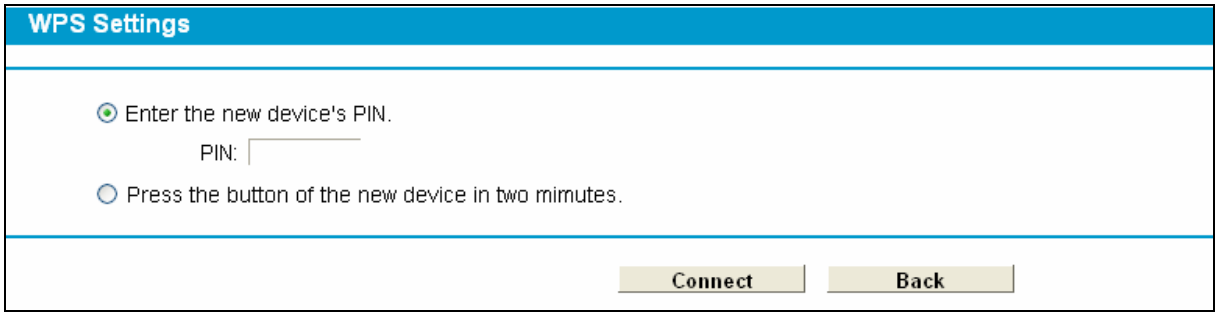


Figure 4-28

Step 2: Enter the PIN number from the client device in the field on the above WPS screen. Then click **Connect** button.

Step 3: "**Connect successfully**" will appear on the screen of Figure 4-28, which means the client device has successfully connected to the Modem Router.

III. Enter the Modem Router's PIN on your client device

Use this method if your client device asks for the Modem Router's PIN number.

Step 1: On the client device, enter the PIN number listed on the Modem Router's Wi-Fi Protected Setup screen. (It is also labeled on the bottom of the Modem Router.)

Step 2: The Wi-Fi Protected Setup LED flashes for two minutes during the Wi-Fi Protected Setup process.

Step 3: When the WPS LED is on, the client device has successfully connected to the Modem Router.

Step 4: Refer back to your client device or its documentation for further instructions.

Note:

1) The WPS LED on the Modem Router will light green for five minutes if the device has been successfully added to the network.

2) The WPS function cannot be configured if the Wireless Function of the Modem Router is disabled. Please make sure the Wireless Function is enabled before configuring the WPS.

4.6.3 Wireless Security

Choose menu "**Wireless**"→" **Wireless Security**", you can configure the security settings of your wireless network.

There are three wireless security modes supported by the Modem Router: WEP (Wired Equivalent Privacy), WPA-PSK (Pre-Shared Key), WPA2-PSK (Pre-Shared Key).

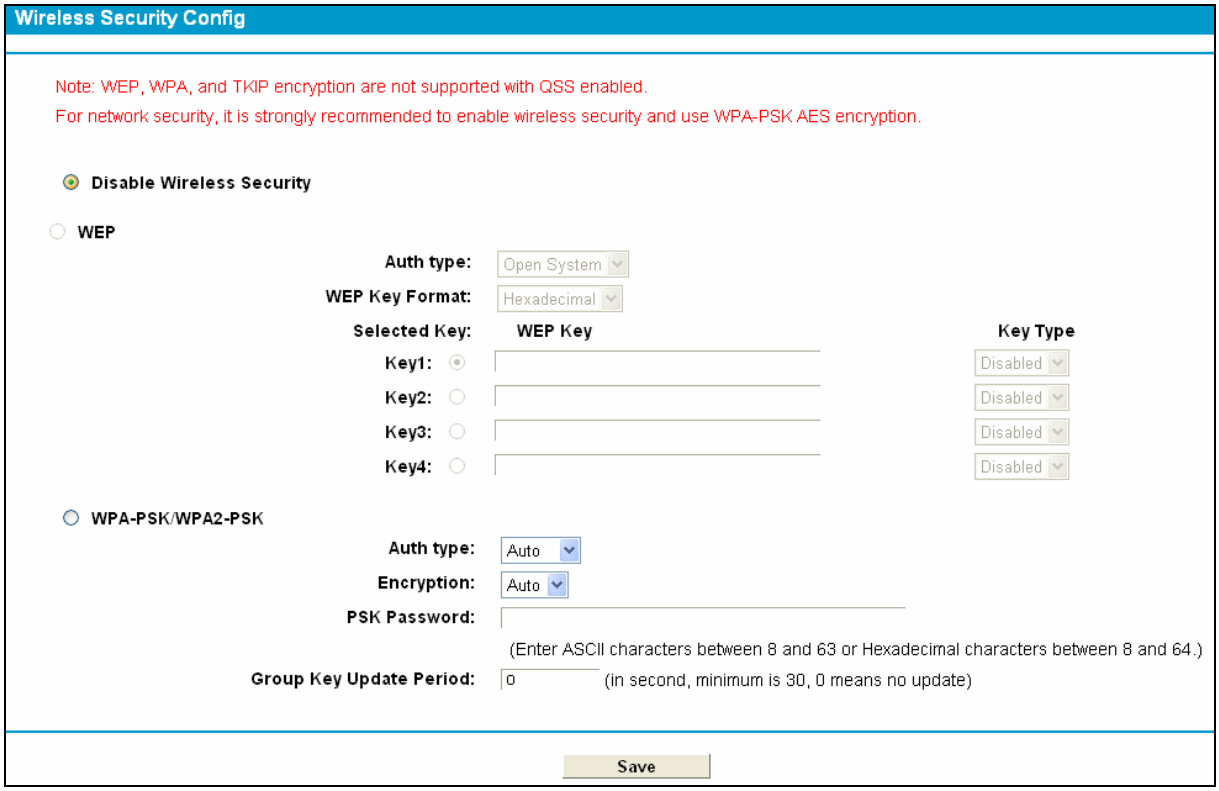


Figure 4-29

- **Disable Wireless Security:** If you do not want to use wireless security, check this radio button. But it's strongly recommended to choose one of the following modes to enable security.

➢ **WEP:** It is based on the IEEE 802.11 standard. If you check this radio button, you will find a notice in red as show in Figure 4-29.

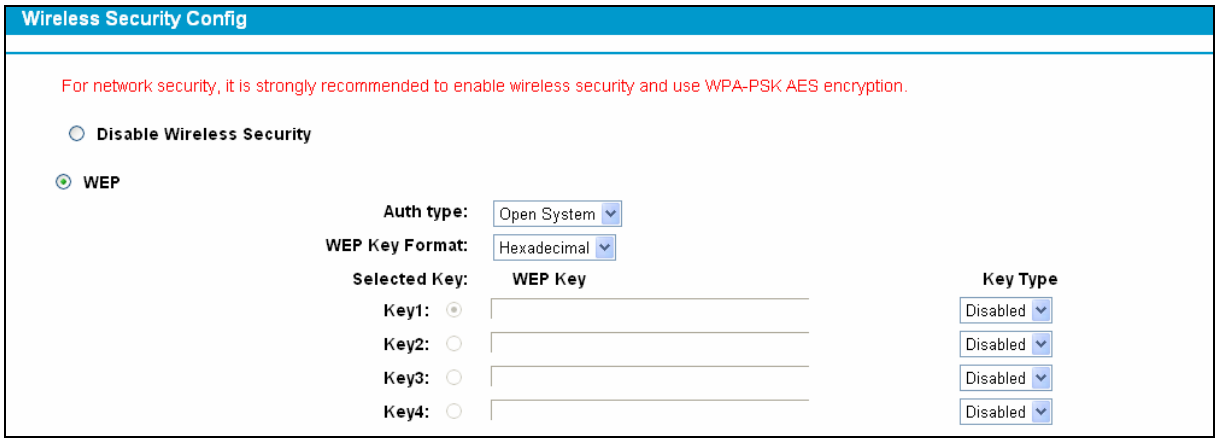


Figure 4-30

- **Auth Type -** you can choose the type for the WEP security on the drop-down list. The default setting is **Automatic**, which can select **Shared Key** or **Open System** authentication type automatically based on the wireless station's capability and request.
- **WEP Key Format - Hexadecimal** and **ASCII** formats are provided here. **Hexadecimal** format stands for any combination of hexadecimal digits (0-9, a-f, A-F) in the specified length. **ASCII** format stands for any combination of keyboard characters in the specified length.
- **WEP Key -** Select which of the four keys will be used and enter the matching WEP key that you create. Make sure these values are identical on all wireless stations in your network.
- **Key Type -** You can select the WEP key length (64-bit, or 128-bit, or 152-bit.) for encryption. "Disabled" means this WEP key entry is invalid.

  64-bit - You can enter 10 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not promoted) or 5 ASCII characters.

  128-bit - You can enter 26 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not promoted) or 13 ASCII characters.

  152-bit - You can enter 32 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not promoted) or 16 ASCII characters.

☞ **Note:**

If you do not set the key, the wireless security function is still disabled even if you have selected Shared Key as Authentication Type.

➢ **WPA-PSK /WPA2-PSK:** It's based on Radius Server.

- **Auth type -** you can choose the version of the WPA security on the drop-down list. The default setting is **Auto**, which can select **WPA (**Wi-Fi Protected Access) or **WPA2 (**WPA version 2) automatically based on the wireless station's capability and request.
- **Encryption -** You can select either **Auto**, or **TKIP** or **AES.**
- **PSK Password -** You can enter ASCII characters between 8 and 63 characters or 8 to 64 Hexadecimal characters.

- **Group Key Update Period -** Specify the group key update interval in seconds. The value should be 30 or above. Enter 0 to disable the update.

Be sure to click the **Save** button to save your settings on this page.

4.6.4 Wireless MAC Filtering

Choose menu "**Wireless**" → "**MAC Filtering**", you can control the wireless access by configuring the **Wireless MAC Filtering** function, shown in Figure 4-31.

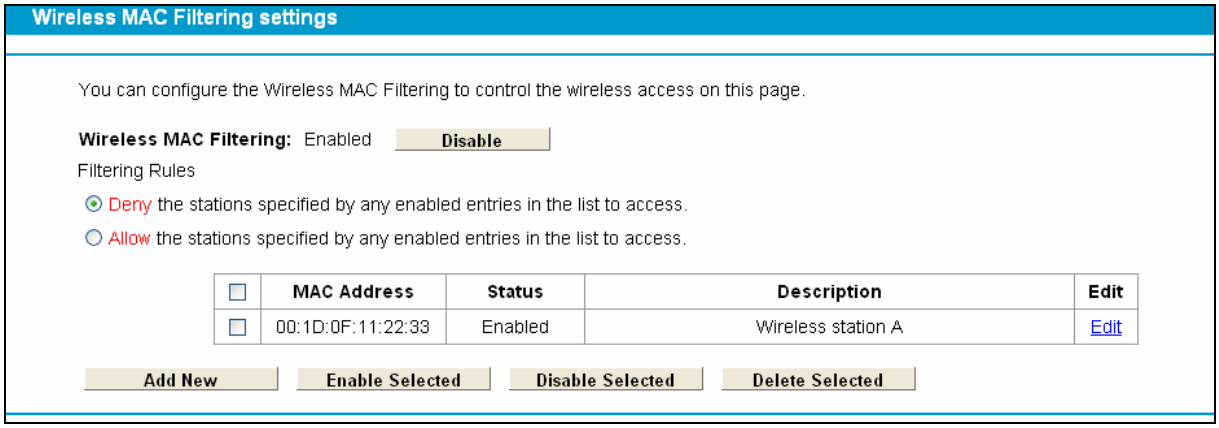


Figure 4-31

To filter wireless users by MAC Address, click **Enable**. The default setting is **Disabled**.

- **MAC Address:** The wireless station's MAC address that you want to filter.
- **Status:** The status of this entry, either **Enabled** or **Disabled**.
- **Description:** A simple description of the wireless station.

To Add a Wireless MAC Address filtering entry, click the **Add New** button. The following page will appear, shown in Figure 4-32:

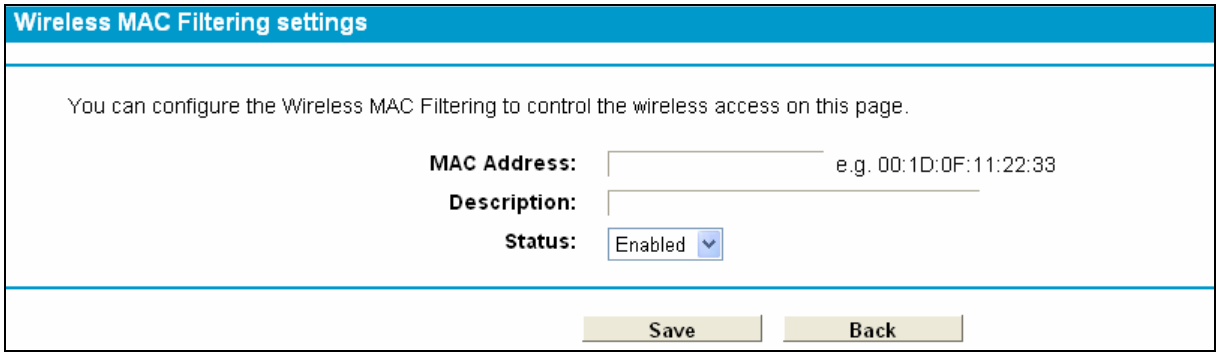


Figure 4-32

To add or modify a MAC Address Filtering entry, follow these instructions:

1. Enter the appropriate MAC Address into the **MAC Address** field. The format of the MAC Address is XX:XX:XX:XX:XX:XX (X is any hexadecimal digit). For example: 00:1D:0F:11:22:33.
2. Give a simple description for the wireless station in the **Description** field. For example: Wireless station A.
3. Select **Enabled** or **Disabled** for this entry on the **Status** drop-down list.

4. Click the **Save** button to save this entry.

To edit or delete an existing entry:

1. Click the **Edit** in the entry you want to modify.
2. Modify the information.
3. Click the **Save** button.

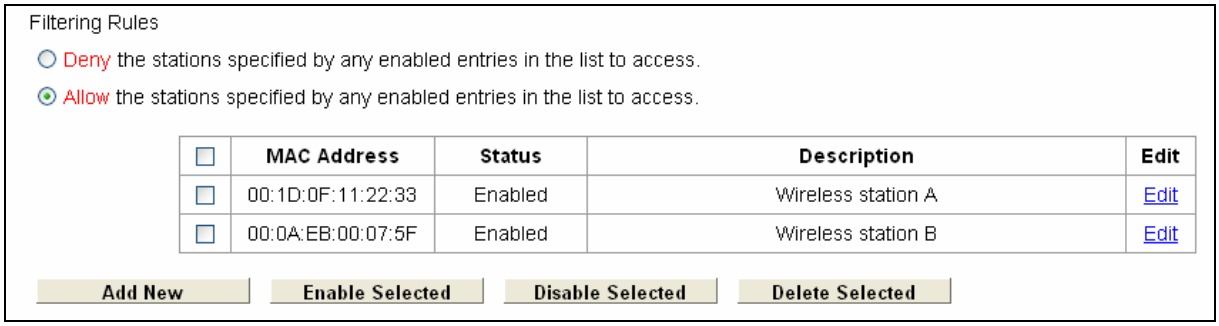
Click the **Enable/ Disabled Selected** button to make selected entries enabled or disabled.

Click the **Delete Selected** button to selected entries.

For example: If you desire that the wireless station A with MAC address 00:1D:0F:11:22:33 and the wireless station B with MAC address 00:0A:EB:00:07:5F are able to access the Modem Router, but all the other wireless stations cannot access the Modem Router, you can configure the **Wireless MAC Address Filtering** list by following these steps:

1. Click the **Enable** button to enable this function.
2. Select the radio button "**Allow the stations specified by any enabled entries in the list to access**" for **Filtering Rules**.
3. Delete all or disable all entries if there are any entries already.
4. Click the **Add New** button.
   1) Enter the MAC address 00:1D:0F:11:22:33/00:0A:EB:00:07:5F in the **MAC Address** field.
   2) Enter wireless station A/B in the **Description** field.
   3) Select **Enabled** in the **Status** drop-down list.
   4) Click the **Save** button.
   5) Click the **Back** button.

The filtering rules that configured should be similar to the following list:



4.6.5 Wireless Advanced

Choose menu "**Wireless**"→"**Wireless Advanced**", you can configure the advanced settings of your wireless network.

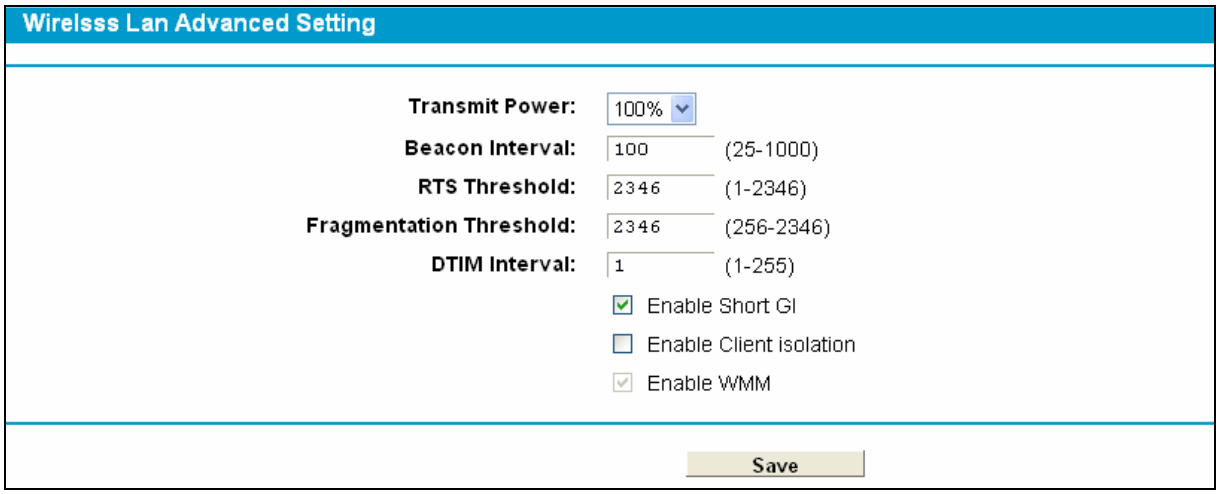


Figure 4-33

- **Transmit Power:** Here you can specify the transmit power of Modem Router. You can select High, Middle or Low which you would like. High is the default setting and is recommended.
- **Beacon Interval:** Enter a value between 25-1000 milliseconds for Beacon Interval here. The beacons are the packets sent by the Modem Router to synchronize a wireless network. Beacon Interval value determines the time interval of the beacons. The default value is 100.
- **RTS Threshold:** Here you can specify the RTS (Request to Send) Threshold. If the packet is larger than the specified RTS Threshold size, the Modem Router will send RTS frames to a particular receiving station and negotiate the sending of a data frame. The default value is 2346.
- **Fragmentation Threshold:** This value is the maximum size determining whether packets will be fragmented. Setting the Fragmentation Threshold too low may result in poor network performance because of excessive packets. 2346 is the default setting and is recommended.
- **DTIM Interval:** This value determines the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the Modem Router has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. You can specify the value between 1-255 Beacon Intervals. The default value is 1, which indicates the DTIM Interval is the same as Beacon Interval.
- **Enable Short GI:** This function is recommended for it will increase the data capacity by reducing the guard interval time.
- **Enabled Client isolation:** This function can isolate wireless stations on your network from each other. Wireless devices will be able to communicate with the Modem Router but not with each other. To use this function, check this box. Client isolation is disabled by default.
- **Enable WMM: WMM** function can guarantee the packets with high-priority messages being transmitted preferentially. It is strongly recommended.

Note:

If you are not familiar with the setting items in this page, it's strongly recommended to keep the provided default values; otherwise it may result in lower wireless network performance.

4.6.6 Wireless Status

Choose menu "**Wireless**"→"**Wireless Status**", you can see the MAC Address, Current Status, Received Packets and Sent Packets for each connected wireless station.

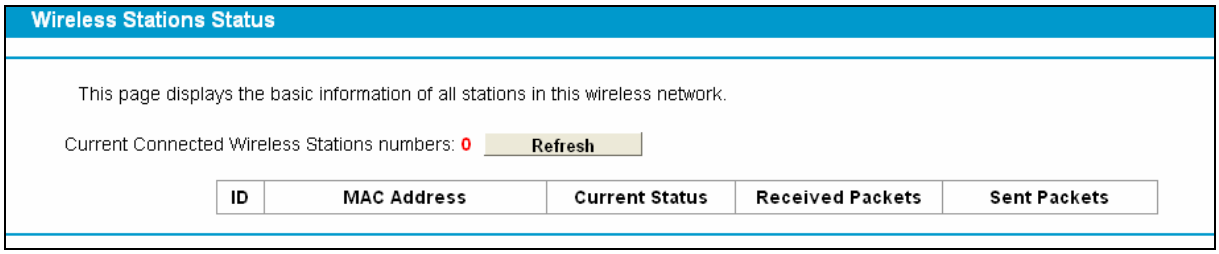


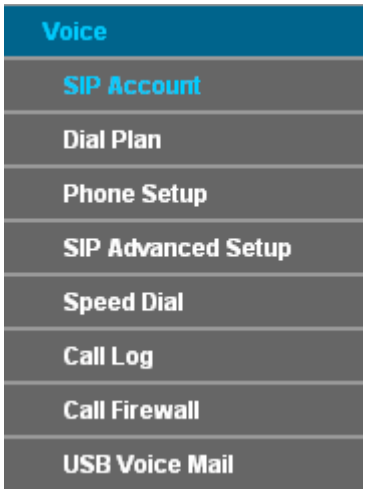
Figure 4-34

- **MAC Address:** The connected wireless station's MAC address
- **Current Status:** The connected wireless station's running status, one of **STA-AUTH/ STA-ASSOC/ STA-JOINED/ WPA/ WPA-PSK/ WPA2/ WPA2-PSK/ AP-UP/ AP-DOWN/ Disconnected**
- **Received Packets:** Packets received by the station
- **Sent Packets:** Packets sent by the station

You cannot change any of the values on this page. To update this page and to show the current connected wireless stations, click on the **Refresh** button.

4.7 Voice

Choose "**Voice**", there are eight submenus under the main menu. Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.



4.7.1 SIP Account

Choose "**Voice**"→"**SIP Account**", you will see the screen similar to Figure 4-35. SIP accounts are necessary for making VoIP calls. This section introduces how to setup the SIP(Session Initiation Protocol) account for your Modem Router.

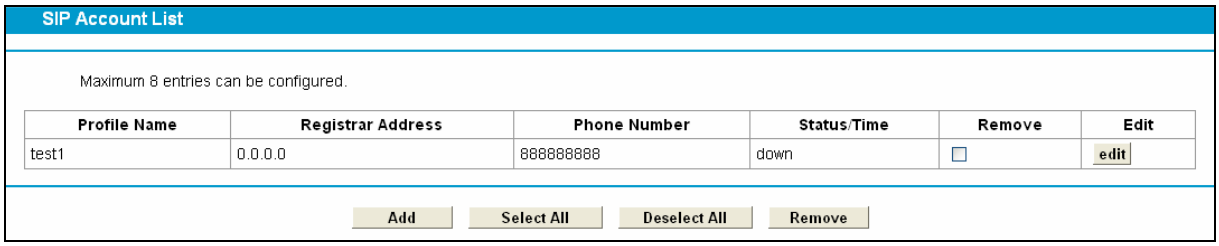


Figure 4-35

- **Profile Name:** Displays the profile name of the account.
- **Registrar Address:** Displays the IP address of the SIP Registrar server.
- **Phone Number:** Displays the phone number of the account.
- **Status/Time:** Displays the status and registration time of the account. “Down” means that the account has not been registered.
- **Remove:** Check the box and then click the **Remove** button below so that the very account will be deleted.
- **Edit:** Click the **Edit** button to modify the very account.

To set up an SIP account, click the Add button in Figure 4-35. Configure the following parameters in Figure 4-36 and then click the **Save** button. Then an account is added. Please note that the blanks with red asterisk behind are required to be entered.

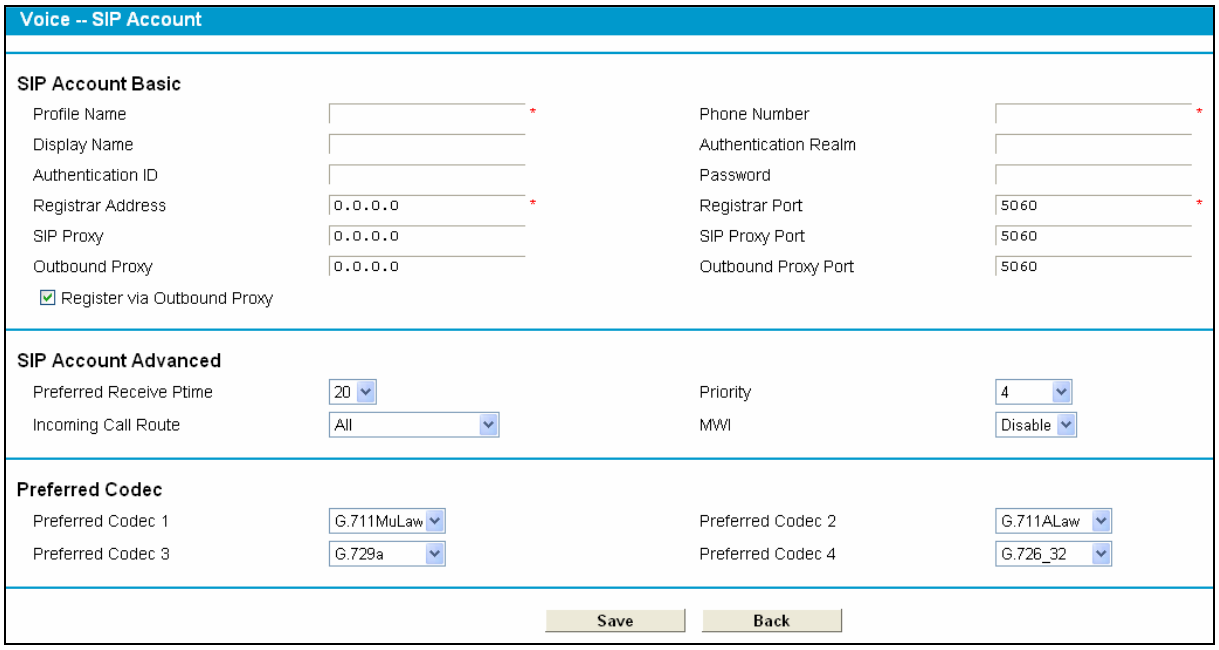


Figure 4-36

SIP Account Basic

- **Profile Name:** Assign a name to identify the profile. Please note that special characters are not allowed.
- **Phone Number:** Enter the phone number of the account you applied.
- **Display Name:** Assign a name for your account. This name is the Caller-ID you want to be displayed on your friend’s display panel, which can let your friend easily know who is calling. Please note that special characters are not allowed.

- **Authentication ID:** Enter the name or number used for SIP Authorization with SIP Registrar. This value is provided by your service provider. If it's not provided, keep the default value.
- **Password:** This parameter, given by your service provider, holds the password used for authentication within VoIP SIP registrar.
- **Registrar Address:** Set the IP address of the SIP Registrar server, which is provided by your service provider.
- **Registrar Port:** Specify the port of the VoIP SIP registrar on which it will listen for register requests from VoIP device.
- **SIP Proxy:** Enter the SIP proxy if it's provided, or keep the default value.
- **SIP Proxy Port:** Enter the SIP proxy port if it's provided, or keep the default value.
- **Outbound Proxy:** Indicate the VoIP SIP outbound proxy server IP address. This parameter is very useful when VoIP device is behind a NAT, say the Modem Router you use connects to Internet by other device. Keep the default if it's not provided by your service provider.
- **Outbound Proxy Port:** Specify the port of the VoIP SIP outbound proxy on which it will listen for messages. Keep the default value if it's not provided by your service provider.

SIP Account Advanced

- **Preferred Receive Ptime:** Ptime, short for packet time, refers to the time interval for a voice packet to be sent by the remote caller. The unit is ms (millisecond). Usually the default value 20ms is OK.
- **Priority:** Select a priority for this account. This priority is useful when more than one account is added in this Modem Router.
- **Incoming Call Route:** Select which line the incoming VoIP call will be routed to.
  - **None:** All incoming VoIP calls will be denied.
  - **Phone 1/Phone 2:** The incoming call will be routed to either Phone1 or Phone 2 randomly.
  - **Idle:** The incoming call will be routed to idle phone in priority.
  - **All:** The incoming call will be routed to both Phone1 and Phone 2 synchronously.
  - **PSTN 2nd Stage Dial:** The incoming call requires second stage dial. This function is applicable on the FXO ports that function as a bridge between VoIP call and PSTN. The user can remotely use the PSTN line to initial a call.
- **MWI:** MWI is short for Message Waiting Indicator. Enable this option, so there will be indications when voice message are received.
- **Preferred Codec (1~4):** Codec is known as Coder-Decoder which is used for data signal conversion. Each codec uses a different bandwidth and hence provides different levels of voice quality. The default codec settings are shown in the corresponding field for your reference. Preferred Codec1 owns the top priority. You can change the value if you are provided with this parameter; otherwise leave it default.

4.7.2 Dial Plan

Choose "**Voice**"→"**Dial Plan**"**,** you will see the screen similar to Figure 4-37. This section includes Dial Plan List, Forbidden Call and Emergency call. The function allows users to set rules for

outgoing calls.

4.7.2.1 Dial Plan List

Dial plan List allows the Modem Router to use specific defined account or network to make outgoing calls. Prefix number is the key to making a distinction between VoIP and PSTN call. If actual numbers dialed match prefix number defined in the dial plan, the dialed number will be routed to the specified network according to this plan. Besides, operation of stripping prefix, replacing prefix or adding prefix, is helpful for users to make a quick and easy call.

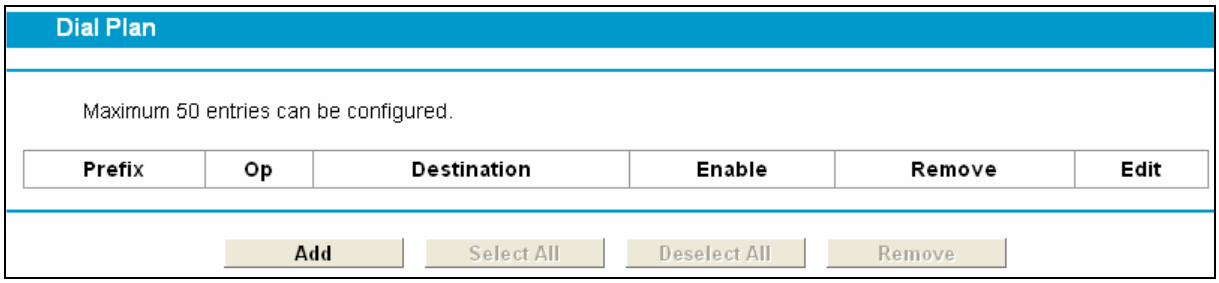


Figure 4-37

- **Prefix:** Displays the prefix of your plan. This prefix refers to the initial digit(s) of the numbers you dial.
- **Op:** Displays the operation of this plan.
- **Destination:** Displays the account or network used for this plan.
- **Enable:** Displays the interface(s) enabled in this plan.
- **Remove:** Check the box and then click the **Remove** button below so that the very plan will be deleted.
- **Edit:** Click the **Edit** button to modify the very plan.

To add a dial plan, click the **Add** button in Figure 4-37. Fill in the following parameters and click the **Save** button in Figure 4-38.

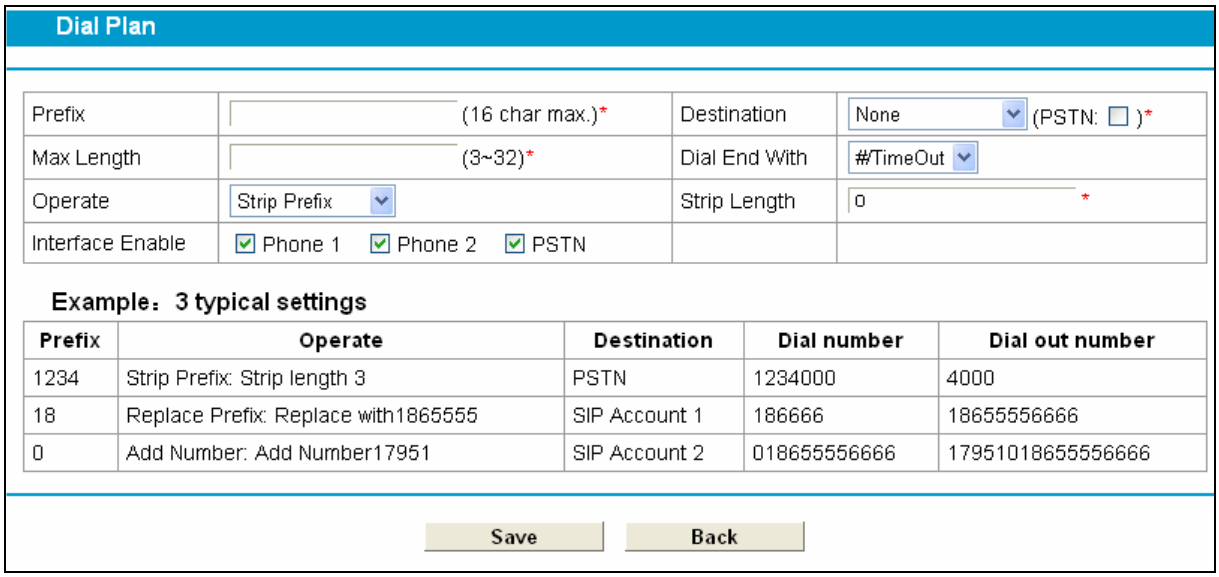


Figure 4-38

- **Prefix:** Set number(s) as the prefix. Up to 16 characters can be entered.

- **Destination:** Both SIP account and PSTN can be selected here. As to which one will be finally used, it depends on not only Destination selected here but also Dial Plan Priority configured on Phone Setup page. Please note that if you want to select a SIP account, you should first add one on SIP Account page; otherwise only NONE is available.
- **Max Length:** Specify the max length of numbers you wish to dial out. The length of the actual dialed number can not exceed the length set here. For example, if the length is set to "6", when you dial "7654321", only "765432" will be sent out.
- **Dial End With:** Ways of indicating when the dialing is finished.

  If "TimeOut" is selected, the dialing will be sent out when timeout starts. The timeout activates when no more digits are dialed in a specific duration;

  If "#" is selected, the dialing will not be sent until "#" is dialed;

  If "#/TimeOut" is selected, the dialing will be sent out when timeout starts or "#" is dialed;

  If "None" is selected, the dialing will not be sent out unless the length of number you dial meets the Max Length.
- **Operate:** Specify a dialing method to make call(s).
  - Strip Prefix – If it is selected, the original phone number will be sent out with the prefix deleted; you can limit the strip length by entering digits in "Strip Length" field.

    Take the 1st dial plan in Figure 4-38 as an example. If you dial 12340000, number 40000 will be dialed out to make a call.
  - Replace Prefix – If it is selected, the original phone number will be sent out with the prefix replaced by what you set in the "Replace With" field.

    Take the 2nd dial plan in Figure 4-38 as an example. If you dial 186666, number 18655556666 will be dialed out to make a call.
  - Add Number – If it is selected, the original phone number will be sent out with what you set in "Add Number" field added ahead.

    Take the 3rd dial plan in Figure 4-38 as an example. If you dial 018655556666, number 1795101865555666 will be dialed out to make a call.
- **Interface Enable**: You can check any box to enable interface(s). Numbers matching prefix in Dial Plan List can only be dialed out through the selected interface(s).

4.7.2.2 Forbidden Call

Choose "**Voice**"→"**Dial Plan**" →"**Forbidden Call**", you will see the screen similar to Figure 4-39. Forbidden Call makes it possible for administrators to control user's access to the voice service.

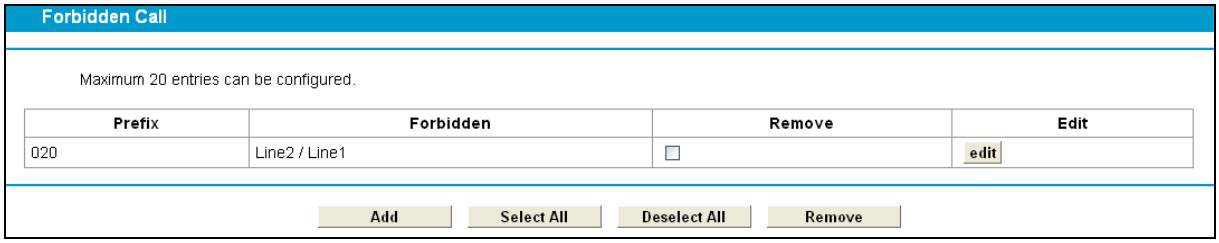


Figure 4-39

- **Prefix:** Displays the prefix of your plan. This prefix refers to the initial digit(s) of the numbers

you dial.

- **Forbidden:** Displays the interface(s) disabled in this plan.
- **Remove:** Check the box and then click the **Remove** button below so that the very plan will be deleted.
- **Edit:** Click the **Edit** button to modify the very plan.

To add a dial plan, click the **Add** button in Figure 4-39. Fill in the following parameters and click the **Save** button in Figure 4-40.

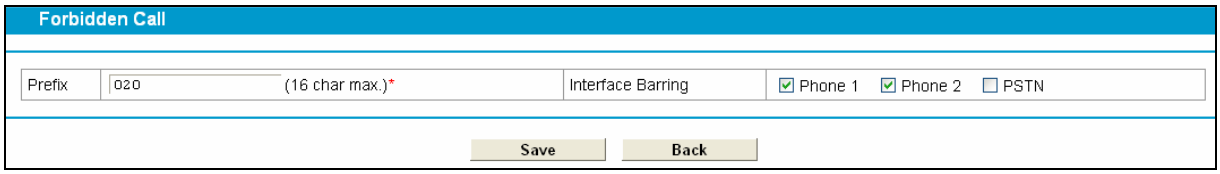


Figure 4-40

- **Prefix:** Set number(s) as the prefix. Up to 16 characters can be entered.
- **Interface Barring:** You can check any box to disable interface(s). Numbers matching prefix in Forbidden Call list are not allowed to be dialed out through the selected interface(s).

For example, if you set a dial plan list in the screen as shown in Figure 4-40, phone numbers starts with '020' can only be dialed out through PSTN line.

4.7.2.3 Emergency Call

Some emergency phone numbers (e.g. 911) can only be dialed out by through PSTN line. This function can make sure emergency calls will be dialed out efficiently.

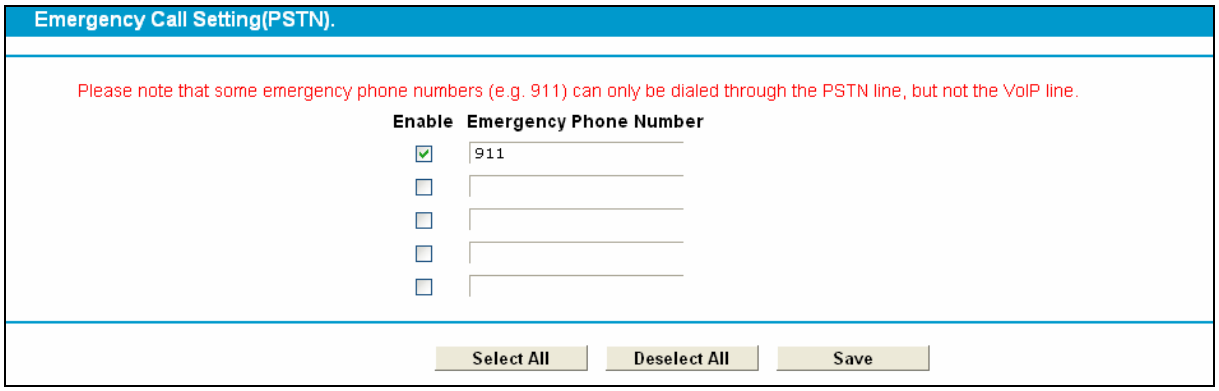

Emergency Call Setting(PSTN).
Please note that some emergency phone numbers (e.g. 911) can only be dialed through the PSTN line, but not the VoIP line.
Enable
Emergency Phone Number
911
Select All
Deselect All
Save

Figure 4-41

- **Enable:** Check the box to enable the very number.
- **Emergency Phone Number:** Type in emergency phone numbers in the blank.

Click the **Save** button to make the configuration take effect.

4.7.3 Phone Setup

Choose "**Voice**"→"**Phone Setup**", you will see the screen similar to Figure 4-42. This section allows you to configure phone settings for phone 1 and phone 2.

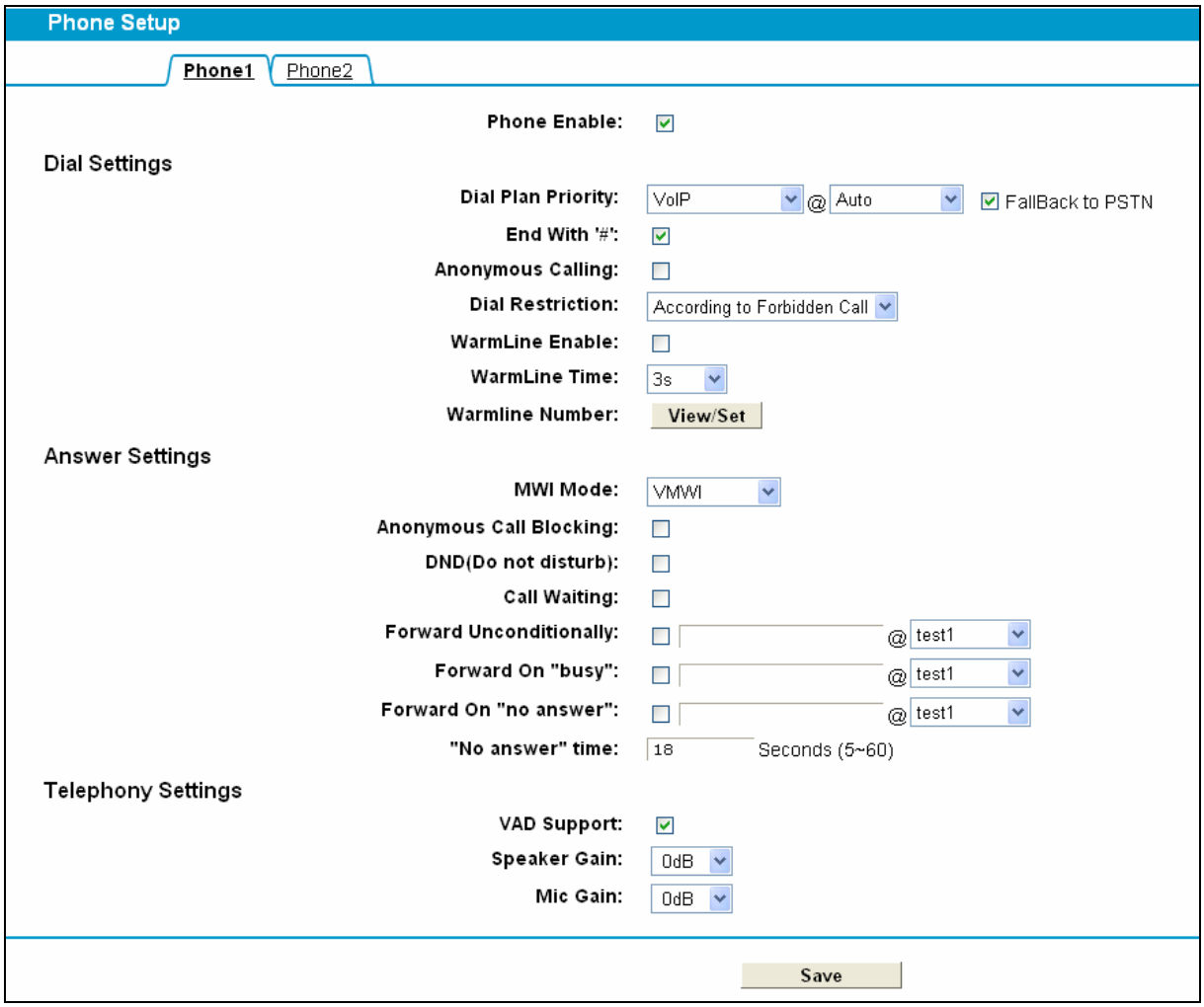


Figure 4-42

➢ **Phone Enable:** Check the box behind to enable the function.

Dial Settings

➢ **Dial Plan Priority:** Define the priority between VoIP and PSTN dial plan.

➢ **Dial Plan Priority:** The parameters configured here determine which network or SIP account to use when making outgoing calls. In the 1st field, there are options of network. Please note if no SIP account is set on SIP Account page, only PSTN network will be available. Otherwise networks available are VOIP, VOIP Preferred and PSTN. If the network selected is not PSTN, you need to choose a SIP account from the 2nd field.

- VOIP & Auto – The Router will always use VoIP network to make calls. As to the account, the one specified in the matched dial plan will be chosen first. Otherwise, the account with top priority will be selected. To view the priority, please go to the screen as shown in Figure 4-36. If “Fallback to PSTN” box is checked, the Router will try PSTN network to make calls after VoIP call fails.
- VOIP & Account X (a certain account) – The Modem Router will always use VoIP network and Account X to make calls.
- PSTN Preferred & Auto – The Router will select the PSTN network and VoIP account to make calls according to your dial plans set on Dial Plan page. If no dial plan is matched with your outgoing call, then PSTN network will be automatically selected.

- PSTN Preferred & Account X (a certain account) – The Router will select the network to make calls according to your dial plans set on Dial Plan page. If VoIP network is selected, the account used will be Account X. But if no dial plan is matched with your outgoing call, then PSTN network will be automatically selected.
- PSTN – The Modem Router will always use PSTN network disregarding your dial plans on Dial Plan page.

➢ **End With '#':** Choose whether to use "#" as the end signal of your dialing or not.

➢ **Anonymous Calling:** Hide the own phone number for each call and it will not be displayed on the remote site. This feature is only available for VoIP calls and disabled by default.

➢ **Dial Restriction:** Choose the pull-down menu to set restriction for outgoing calls.

- **None:** Allow all numbers to be dialed out.
- **All:** Forbid all numbers to be dialed out.
- **According to Forbidden Call:** Numbers will be dialed out according to settings in Forbidden Call.

➢ **WarmLine Enable:** Check the box to enable WarmLine function. So if there is no dialing action after you pick up the phone set, after the warmline time the phone will dial out automatically with the numbers set.

➢ **WarmLine Time:** Choose WarmLine Time from the drop-down list to specify an interval before the phone dials out automatically.

➢ **Warmline Number:** Click "**View/Set**" button to view or set Warmline Number.

Answer Settings

➢ **MWI Mode:** Options available are VMWI and CLID. If you don't know, please consult your service provider.

➢ **Anonymous Call Blocking:** Check the box to deny anonymous incoming calls.

➢ **DND(Do not disturb):** Check the box to deny all incoming calls.

➢ **Call Waiting:** Check the box to enable this function. When the line is busy, the incoming call will be indicated to wait.

➢ **Forward Unconditionally:** If the box behind is checked, all the incoming calls will be forwarded to the number set before @ through selected account. Please note that network or account available here varies with that in Dial Plan Priority field.

➢ **Forward On "busy":** Check the box to enable this function. When the line is busy, all the incoming calls will be forwarded to the number set before @ through selected account. Please note that network or account available here varies with that in Dial Plan Priority field.

➢ **Forward On "no answer"& "No answer" time:** Check the box to enable this function. When there is no answer, all the incoming calls will be forwarded to the number set before @ through selected account when "No answer" time is out. Please note that network or account available here varies with that in Dial Plan Priority field.

Telephony Settings

➢ **VAD Support:** VAD(Voice Activation Detection) prevents transmitting the nature silence to consume the bandwidth. It is also known as Silence Suppression which is a software application that ensures the bandwidth is reserved only when voice activity is activated. It is

enabled by default.

- **Speaker Gain:** Sound Volume control of speaker.
- **Mic Gain:** Sound Volume control of microphone.

4.7.4 Advanced Setup

Choose "**Voice**"→"**Advanced Setup**", you will see the next screen in Figure 4-43.

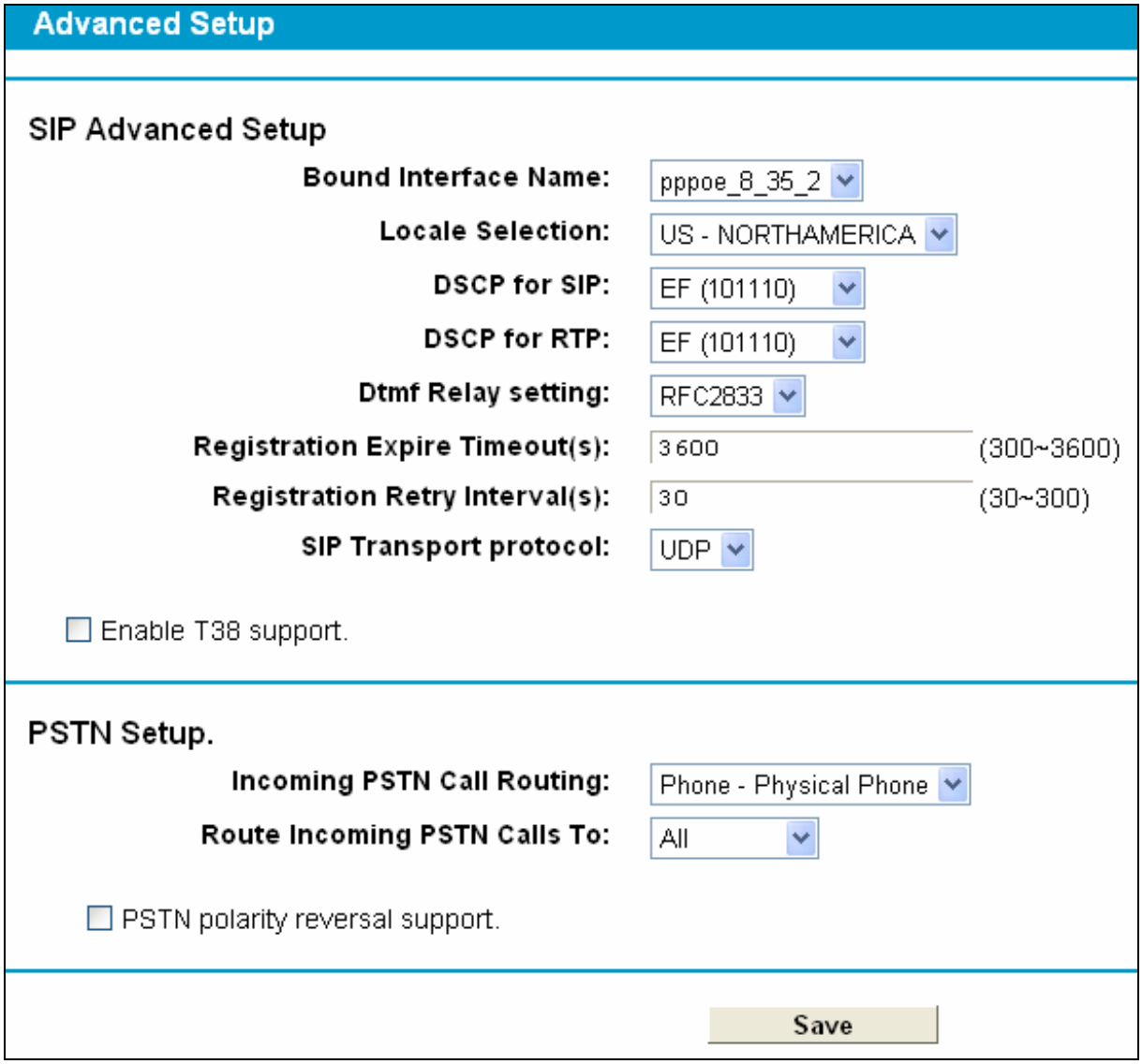


Figure 4-43

SIP Advanced Setup:

- **Bound Interface Name:** Bound Interface decides where to send/receive the VOIP traffic. Easy way to select the interface is to check the location of the SIP server. If it locates some where in the Internet then select **Any_WAN**. If it is on the local network then select **LAN**.
- **Locale Selection:** Select a country where you are located. The Router is embedded with some default parameters according to different countries such as ring tones.
- **DSCP for SIP:** DSCP(Differentiated Services Code Point) is the first 6 bits in the ToS byte. DSCP Marking allows users to assign specific application traffic to be executed in priority by

the next Router based on the DSCP value. Select one DSCP for the SIP. If you are unsure, please always keep the default value.

- **DSCP for RIP:** RIP(Routing Information Protocol), is used for the Modem Router to exchange routing information with neighboring routers to accomplish IP routing. Select one DSCP for the RIP. If you are unsure, please always keep the default value.
- **Dtmf Relay setting:** DTMF is Dual Tone Multi Frequency. Options available are SIPInfo, RFC2833, and InBand. If you are unsure which one to choose, please always keep the default value.
- **SIPInfo** – If it is selected, the Router will capture the DTMF tone and transfer it into SIP form. Then it will be sent to the remote end with SIP message.
  - **RFC2833** – If it is selected, the Router will capture the keypad number you pressed and transfer it into digital form then send to the other side; the receiver will generate the tone according to the digital form it receives. This function is very useful when the network traffic congestion occurs and it still can remain the accuracy of DTMF tone.
  - **InBand** – If it is selected, the Router will send the DTMF tone as audio directly when you press the keypad on the phone.
- **Registration Expire Timeout(s):** Expire time for the registration message sending.
- **Registration Retry Interval(s):** Set the time duration for your SIP Registrar server to keep your registration record. Before the time expires, the Modem Router will send another register request to SIP Registrar again. If you are unsure of it, please always keep the default value.
- **Enable T38 support:** T38 specifies a protocol for transmitting a fax across IP network in real time. It allows the transfer of fax documents in real-time between two standard Group 3 facsimile terminals over the Internet or other networks using IP protocols. It will only function when both sites are support this feature and are enabled.

PSTN Setup

- **Incoming PSTN Calls Routing:** Choose a method for the Router to decide where to route the incoming call on PSTN network.
  - **Phone-Physical Phone** – The Router will route the incoming call according to the physical line selected in “Route Incoming PSTN Calls To” field. For example, if “Idle Phone” is selected, the Router will first judge the status of Phone 1. If it is free, then the incoming call will be routed to Phone 1. Otherwise, the Router will go on judging the status of Phone 2.
  - **VoIP-VoIP call** – The Router will route the incoming call according to the SIP number and account set in “SIP URI of PSTN endpoint” field. For example, if “2654321@test1” is input, the Router will directly route the incoming call to 2654321 through test1. The SIP number and account can be a remote one, say a friend’s SIP number and account.

    Besides, VoIP-VoIP call allows second dialing when the SIP number but not account is left blank, for example “@test1”. This function is applicable on the FXO ports that function as a bridge between VoIP call and PSTN. The user can remotely use the VoIP line to initial a call.
- **PSTN polarity reversal support:** This feature is disabled by default. If you are unsure of it, please always keep the default.

4.7.5 Speed Dial

Choose "**Voice**"→"**Speed Dial**", you will see the screen as shown in Figure 4-44. This section introduces how to configure Speed Dial for your account.

Speed Dial comes to store frequently used telephone numbers and to make your dial more convenient. It allows you to make a call by pressing a short number and the pound sigh # on the phone keypad instead of the original number.

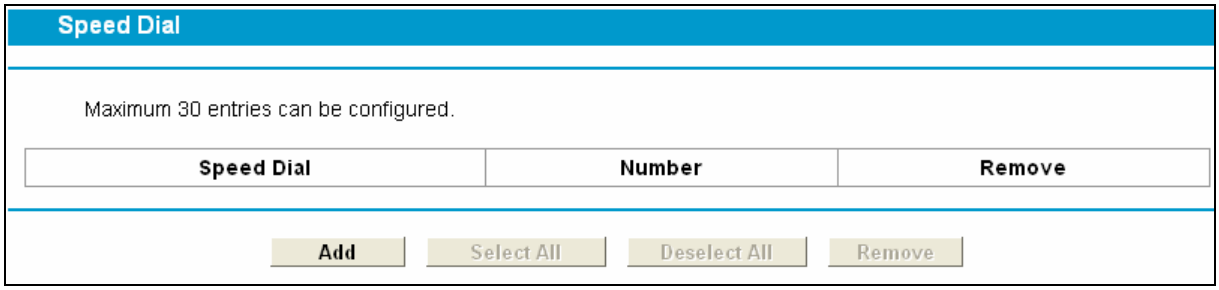


Figure 4-44

To add a Speed Dial entry, click the **Add** button and you will see the screen as shown in Figure 4-45. Fill in the following parameters and then click the Save button.

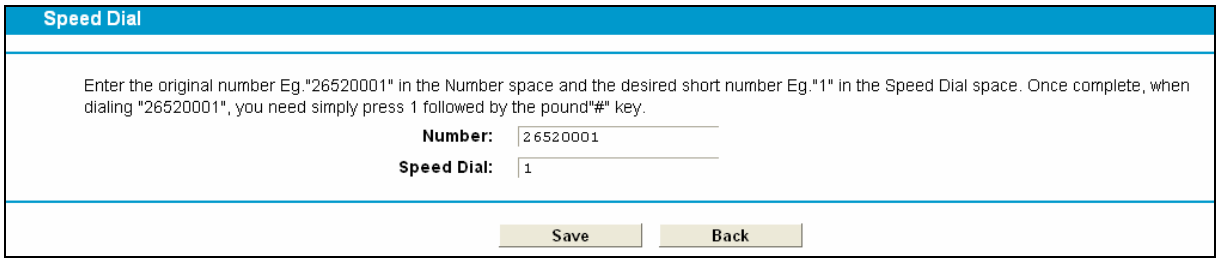

Speed Dial
Enter the original number Eg."26520001" in the Number space and the desired short number Eg."1" in the Speed Dial space. Once complete, when dialing "26520001", you need simply press 1 followed by the pound"#" key.
Number: 26520001
Speed Dial: 1
Save
Back

Figure 4-45

- **Number:** Enter a phone number.
- **Speed Dial:** Enter a number from 0~99.

Click the **Save** button, you will go back to the previous page and see the following list as shown in Figure 4-46.

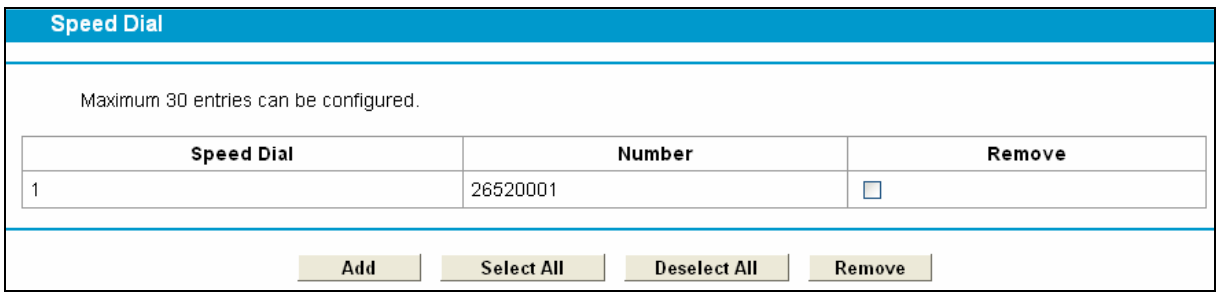


Figure 4-46

Click the **Save** button to make the configuration take effect. If you want to delete the entry, check the **Remove** box first, and then click the **Remove** button.

4.7.6 Call Log

Choose "**Voice**"→"**Call Log**", you will see the screen as shown in Figure 4-47. This function allows you to view call logs and configure call log options.

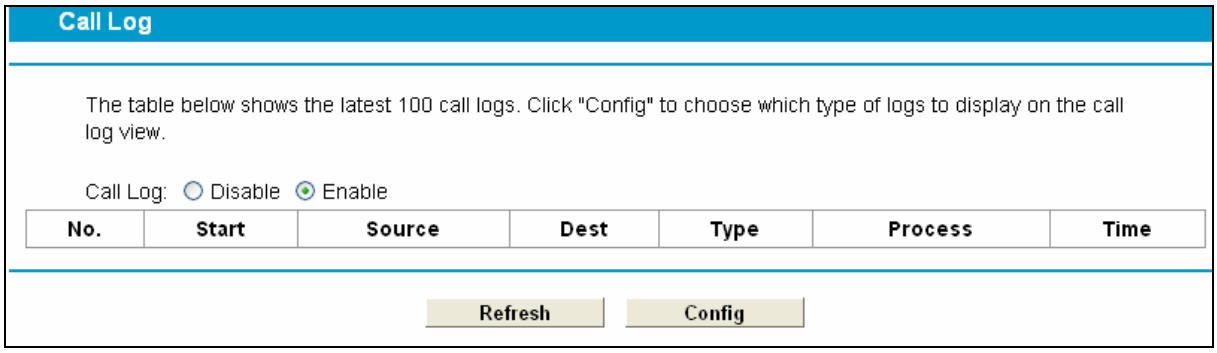


Figure 4-47

- **Call Log:** Check the Enable if you want to make this function take effect, otherwise check the Disable.
- **Start:** Beginning time of the call.
- **Source:** Caller ID, either phone number or IP address.
- **Dest:** Callee ID, either phone number or IP address.
- **Type:** Call types, including Incoming (VoIP), Incoming (PSTN), Outgoing (VoIP) and Outgoing (PSTN).
- **Process:** Process types, including Connected, Local forward, Remote forward, Local transfer, Remote transfer, Conference and Unconnected.
- **Time:** Total call time.

To configure the view of call log, click the **Config** button and you will see the screen as shown in Figure 4-48. This page displays all the call types and process types. You can choose some of them or all of them. Check the boxes before the corresponding options which you desire to view and click the **Save** button to make the configuration take effect.

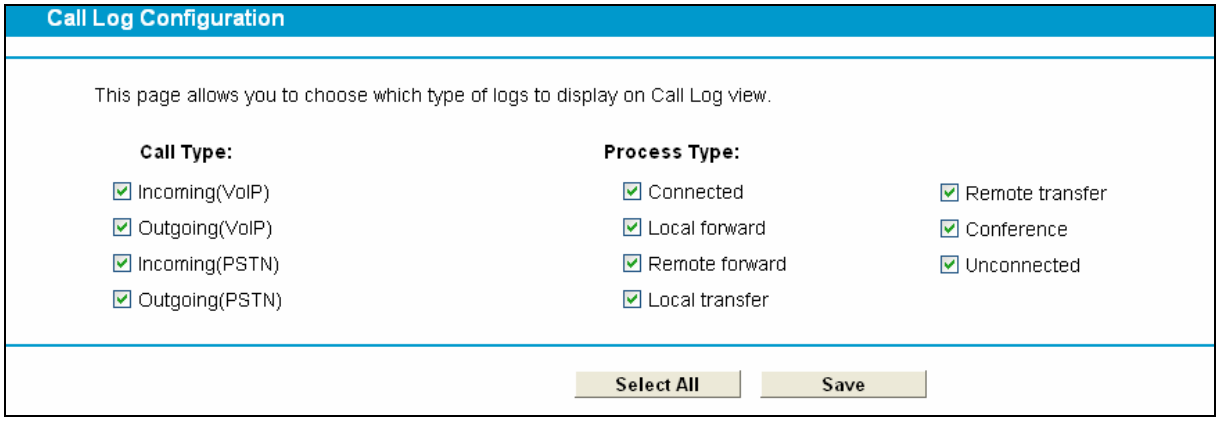


Figure 4-48

4.7.7 Call Firewall

Choose "**Voice**"→"**Call Firewall**", you will see the screen as shown in Figure 4-49. Call Firewall can be used to control incoming calls. This section introduces how to configure the Call Firewall.

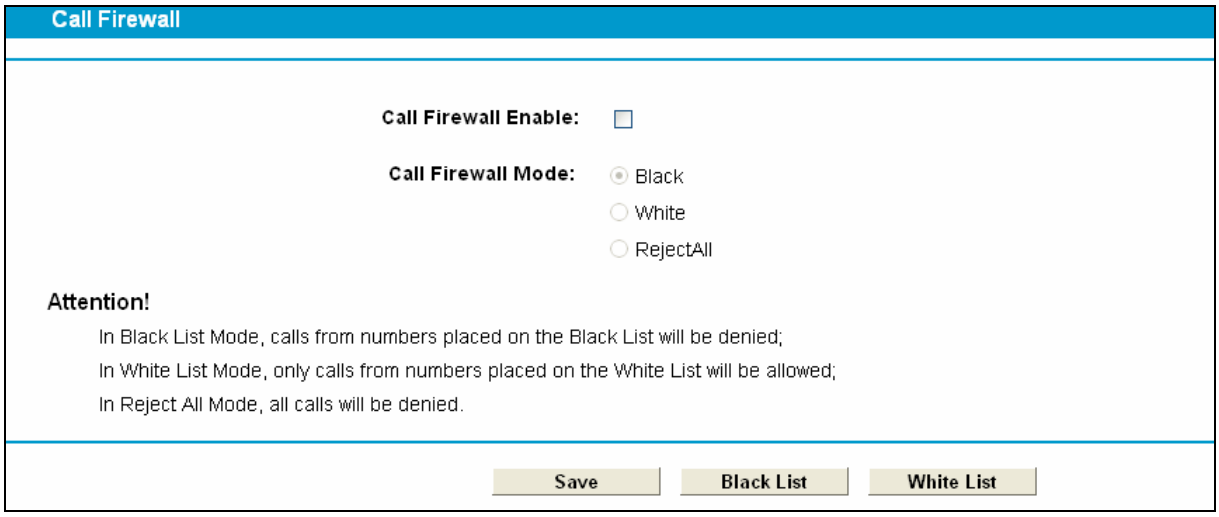

Call Firewall
Call Firewall Enable:
Call Firewall Mode:
Black
White
RejectAll
Attention!
In Black List Mode, calls from numbers placed on the Black List will be denied;
In White List Mode, only calls from numbers placed on the White List will be allowed;
In Reject All Mode, all calls will be denied.
Save
Black List
White List

Figure 4-49

- **Call Firewall Enable:** Check the box if you want to make the Call Firewall take effect.
- **Black:** Check the **Black** box to enable Black List mode. Calls from numbers placed in the Black List will be denied.
- **White**: Check the **White** box to enable White List mode. Only calls from numbers placed in the White List will be allowed.
- **RejectAll:** Check the **RejectAll** box to enable Reject All mode. All incoming calls will be denied.

To configure the Black List, choose "**Call Firewall**"→"**Black List**" on the left menu or click the **Black List** button on screen as shown in, you will see the screen as shown in Figure 4-50.

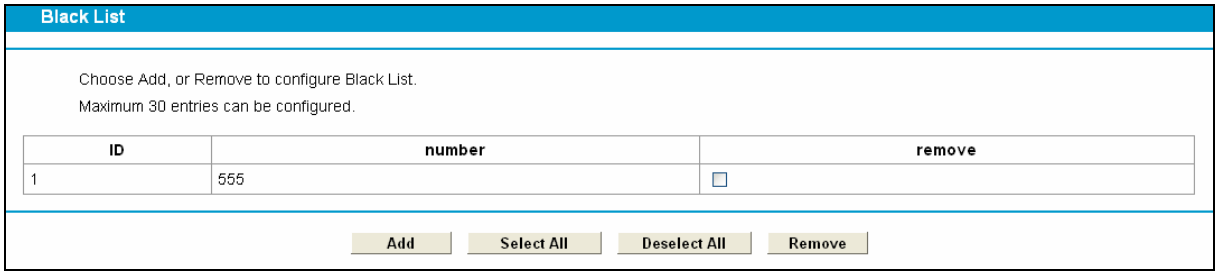


Figure 4-50

To add a new entry, click the **Add** button and you will see the screen as shown in Figure 4-51.

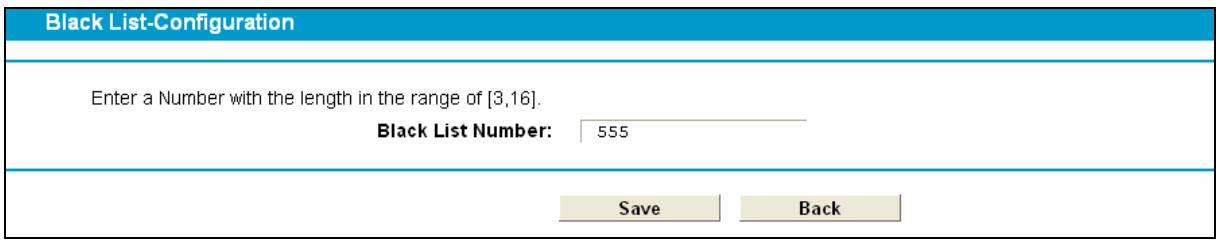


Figure 4-51

Enter a number with the length in the range of [3, 16]in the field of **Black List Number** and Click the **Save** button to make the configuration take effect, then you will go back to the previous page and see the following list as shown in Figure 4-50. If you want to delete the entry, check the **Remove** box first and then click the **Remove** button.

To configure the White List, choose "**Call Firewall**" →"**White List**" on the left menu or click the **White List** button on the screen as shown in, then you will see the screen as shown in Figure 4-52.

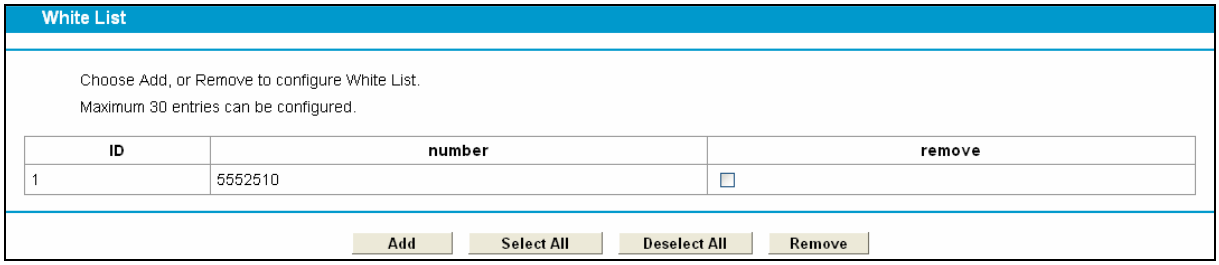


Figure 4-52

To add a new entry, click the **Add** button and you will see the screen as shown in Figure 4-53.

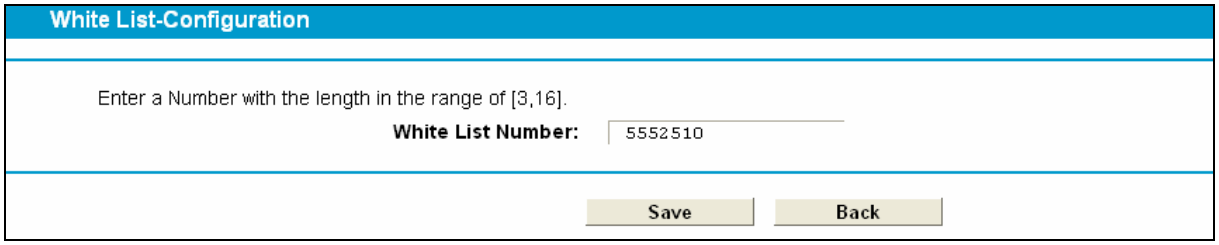


Figure 4-53

Enter a number with the length in the range of [3, 16] in the field of **White List Number** and click the **Save** button to make the configuration take effect, then you will go back to the previous page and see the following list as shown in Figure 4-52. If you want to delete the entry, check the **Remove** box first and then click the **Remove** button.

☞ **Note:**

Partial matching rule is applied here, so this function works for all the incoming call numbers that start with the number you have configured in the Black List or the White List. For example, if the number you have configured in the Black List is 555, with Black List mode enabled the incoming call number 5554510 will be denied.

4.7.8 USB Voice Mail

Choose "**Voice**"→"**USB Voice Mail**", you will see the screen as shown in Figure 4-54. USB Voice mail is used to record voice messages when the call is not answered.

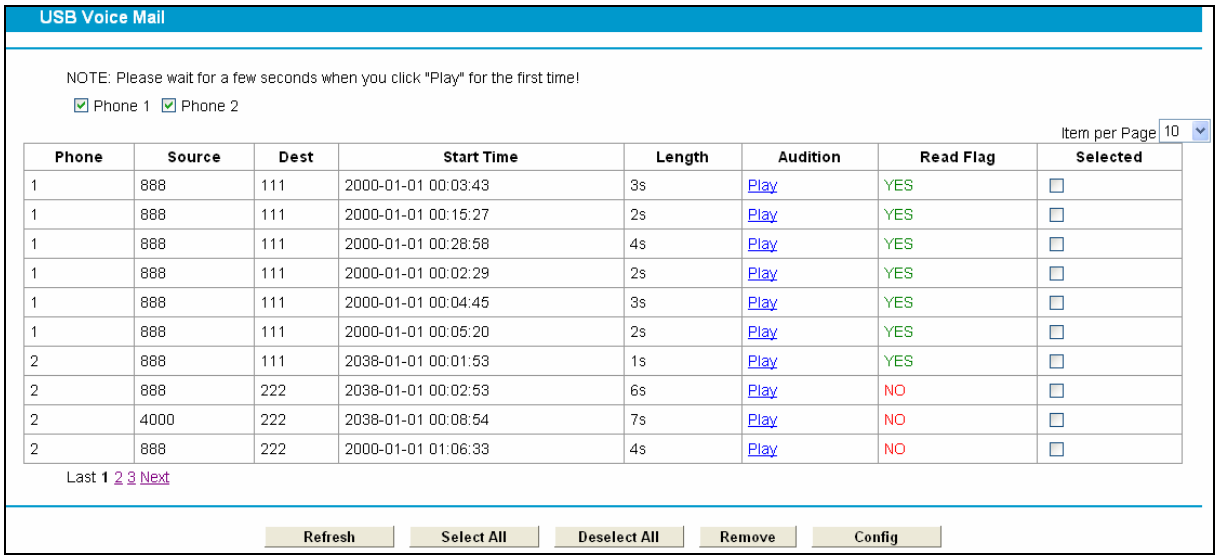

USB Voice Mail
NOTE: Please wait for a few seconds when you click "Play" for the first time!
Phone 1 Phone 2
Item per Page 10
Phone Source Dest Start Time Length Audition Read Flag Selected
1 888 111 2000-01-01 00:03:43 3s Play YES
1 888 111 2000-01-01 00:15:27 2s Play YES
1 888 111 2000-01-01 00:28:58 4s Play YES
1 888 111 2000-01-01 00:02:29 2s Play YES
1 888 111 2000-01-01 00:04:45 3s Play YES
1 888 111 2000-01-01 00:05:20 2s Play YES
2 888 111 2038-01-01 00:01:53 1s Play YES
2 888 222 2038-01-01 00:02:53 6s Play NO
2 4000 222 2038-01-01 00:08:54 7s Play NO
2 888 222 2000-01-01 01:06:33 4s Play NO
Last 1 2 3 Next
Refresh
Select All
Deselect All
Remove
Config

Figure 4-54

- **Phone:** Displays the phone that has voice message.
- **Source:** Displays the source of the voice message, i.e. the remote caller account.
- **Dest:** Displays the destination of the voice message, i.e. the local account.
- **Start Time:** Displays when the voice message starts.
- **Length:** Displays how long the voice message is.
- **Audition:** Click **Play** to listen to the voice message.
- **Read Flag:** Displays whether the voice message has been read or not.
- **Selected:** Check the box to select the corresponding voice message.

To refresh the web page, click **Refresh** button.

To delete a voice message, check the Selected box and then click **Remove** button.

To configure the USB Voice Mail, click **Config** button to enter the web page as shown in Figure 4-55.

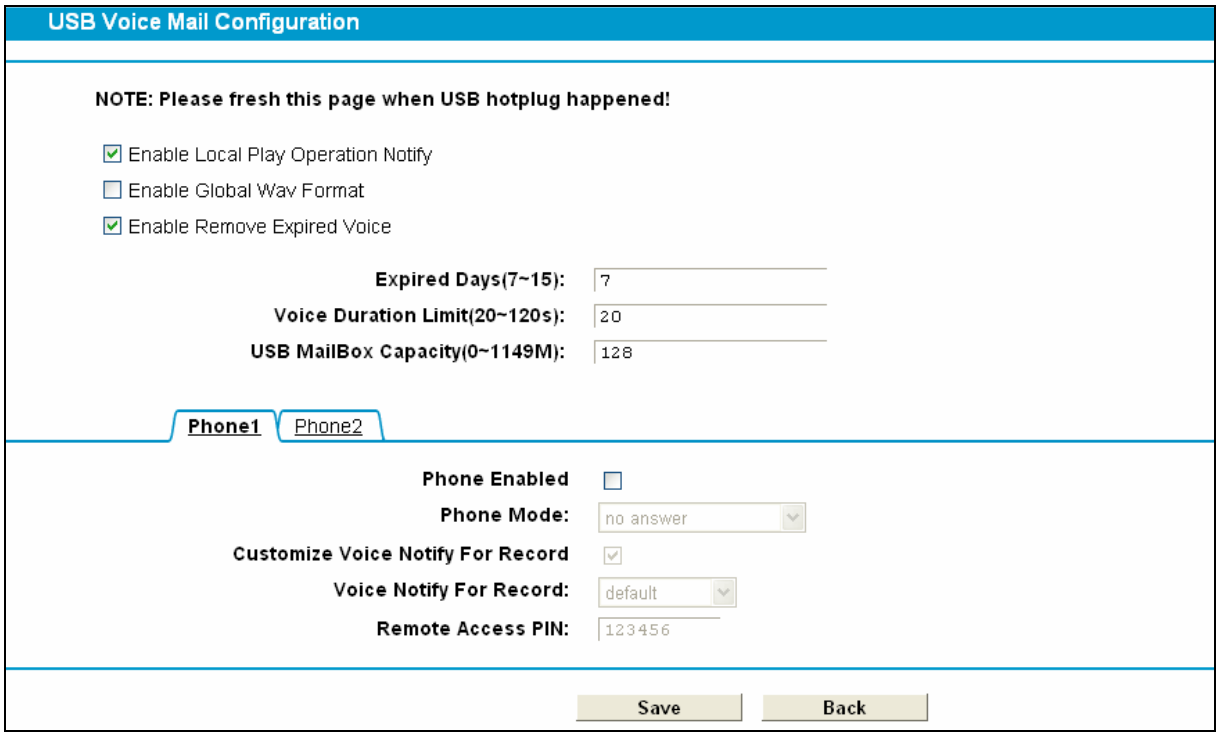


Figure 4-55

- **Enable Local Play Operation Notify:** Check this box so there will be sound indication for operation when you listen to the voice messages. This is enabled by default. If you are very familiar with the operations, you can disable it.
- **Enable Global Wav Format:** Check this box and all the voice message will be saved as wav files in your USB device. It is convenient for users to listen to the voice messages on the computer. Considering the capacity of your USB device, it is disabled by default.
- **Enable Remove Expired Voice:** Check this box and then the expired voice messages will be deleted automatically. Considering the capacity of USB device, it is enabled by default.
- **Expired Days(7~15):** Configure the days that you want the voice messages to be kept.
- **Voice Duration Limit(20~120s):** This option is used to limit the duration of a voice message.
- **USB MailBox Capacity:** Set the capacity for the USB mailbox. Please note that the capacity set should be less than that of the USB device.
- **Phone Enable:** Check the box to enable this function.
- **Phone Mode:** If **no answer** is selected, voice notification will be played when there is no answer. If **unconditionally** is selected, all incoming calls will be directed to voice mail.
- **Customize Voice Notify For Record:** Check the box to enable voice notification customization. To record your own voice notification, press “*30” after picking up your phone set.
- **Voice Notify For Record:** Select to use the default or customized voice notification.
- **Remote Access PIN:** This PIN code is used to listen to the voice messages in a remote place. Operations are as follows.

  1) Call the local phone and wait for the voice notification.

  2) Press “*” before the notification is over.

3) Input the PIN code according to the notification.

4) You can listen to all the new messages after the PIN code is validated.

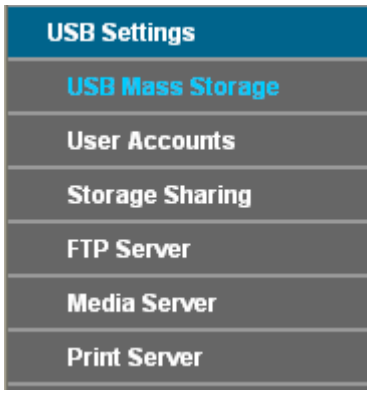
Click **Save** to save your configurations.

Click **Back** to go back to the previous page, i.e. Figure 4-54.

☞ **Note:**

For details about how to configure USB Voice Mail function, please refer to **Quick Installation Guide**.

4.8 USB Settings



There are six submenus under the USB Settings menu, **USB Mass Storage**, **User Accounts**, **Storage Sharing**, **FTP Server**, **Media Server** and **Print Server**. Click any of them, and you will be able to configure the corresponding function.

4.8.1 USB Mass Storage

Choose menu "**USB Settings**" → "**USB Mass Storage**", you can configure a USB disk drive attached to the Modem Router and view volume and share properties such as share name, capacity, status, and action, etc on this page as shown below.

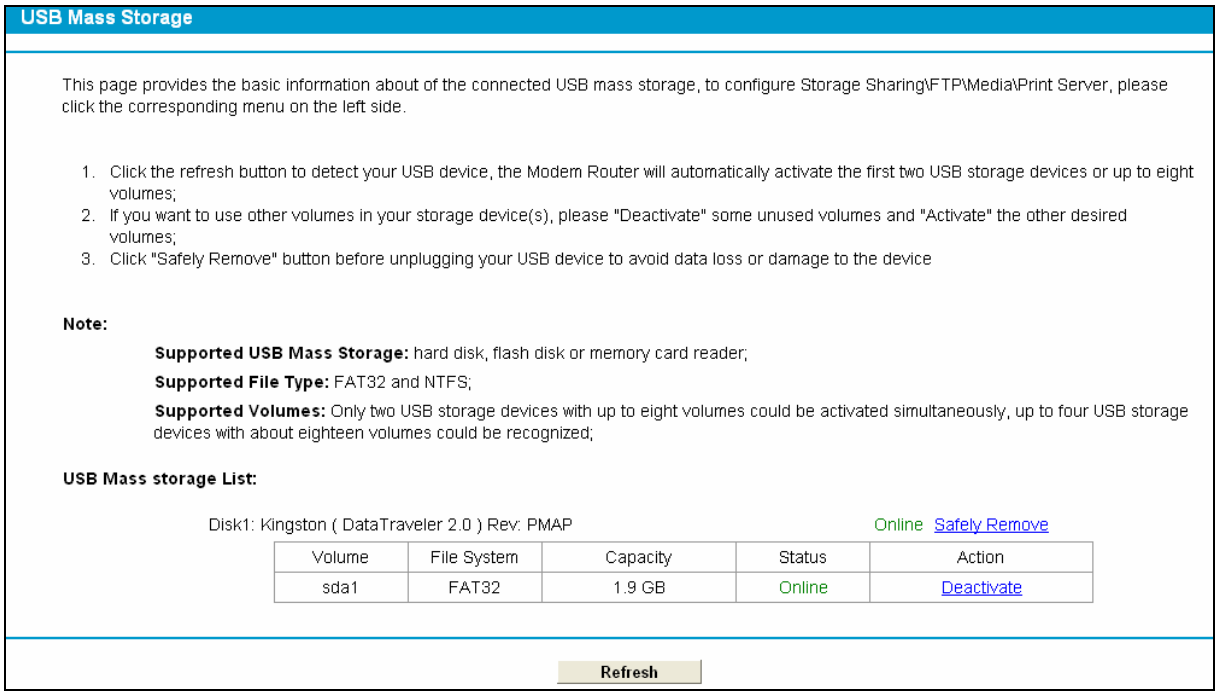

USB Mass Storage
This page provides the basic information about of the connected USB mass storage, to configure Storage Sharing\FTP\Media\Print Server, please click the corresponding menu on the left side.
1. Click the refresh button to detect your USB device, the Modem Router will automatically activate the first two USB storage devices or up to eight volumes;
2. If you want to use other volumes in your storage device(s), please "Deactivate" some unused volumes and "Activate" the other desired volumes;
3. Click "Safely Remove" button before unplugging your USB device to avoid data loss or damage to the device
Note:
Supported USB Mass Storage: hard disk, flash disk or memory card reader;
Supported File Type: FAT32 and NTFS;
Supported Volumes: Only two USB storage devices with up to eight volumes could be activated simultaneously, up to four USB storage devices with about eighteen volumes could be recognized;
USB Mass storage List:
Disk1: Kingston (DataTraveler 2.0) Rev: PMAP
Online
Safely Remove
Volume
File System
Capacity
Status
Action
sda1
FAT32
1.9 GB
Online
Deactivate
Refresh

Figure 4-56

- **Volume:** The volume name of the USB drive the users have access to.
- **File System:** The system of the USB drive.
- **Capacity:** The storage capacity of the USB driver.
- **Status:** Indicates the shared or non-shared status of the volume. **Online** means volume can be shared, while **Offline** means volume can not be shared. If **Deactivate** in Action field is enabled, **Disabled** will be displayed in the Status field, which means volume can not be shared.
- **Action:** When the volume is shared, you can click the **Deactivate** to stop sharing the volume; when volume is non-shared, you can click the **Enable** button to share the volume.

Click **Safely Remove** to safely remove the USB storage device that is connected to USB port.

Note:

Before removing the USB storage device, you should click “Safely Remove” to make sure that all your data have been saved completely. Removing device directly may cause your USB storage device crashed.

4.8.2 User Accounts

You can specify the user name and password for Storage Sharing and FTP Server users on this page. Storage Sharing users can access the folders by entering the following URL into the address field of your browser or Windows Explorer, such as. \\192.168.1.1. FTP Server users can log into the FTP Server via FTP Client.

There are five users here, which provide means to control the access to the USB mass storage by Storage Sharing or FTP. The Super User has the right to read and write to Storage Sharing and FTP Server.

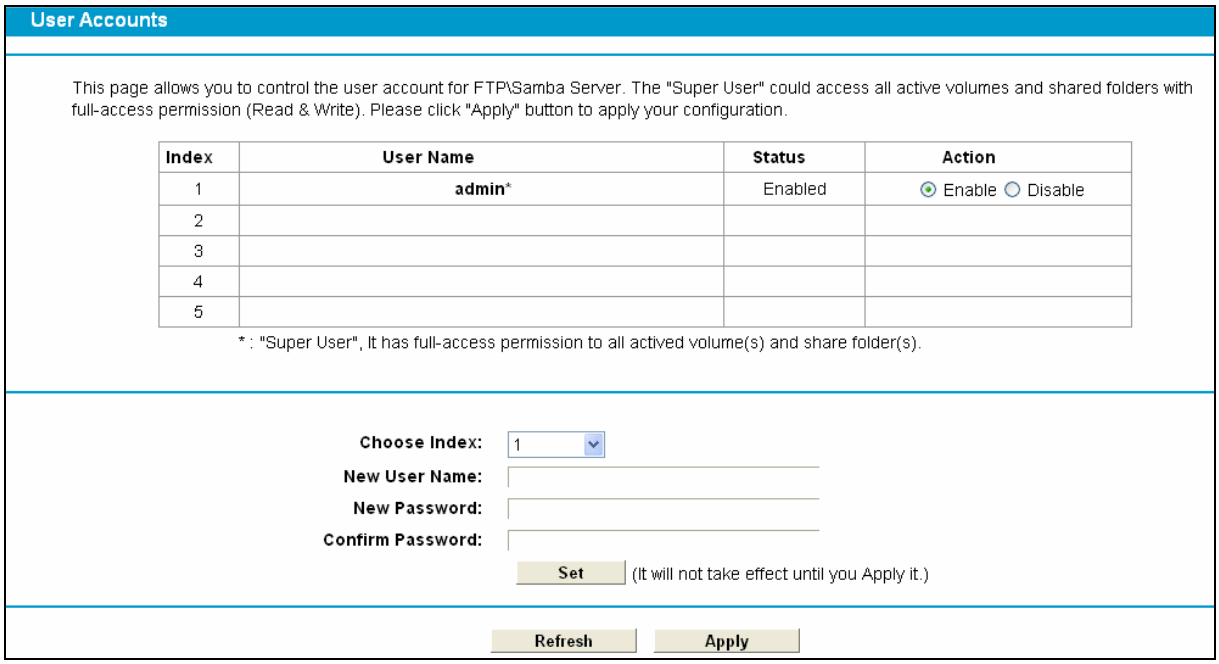


Figure 4-57

To add a new user account, please follow the steps below:

1. Choose the index from the drop-down list of **Choose Index**.
2. Self-define a **New User Name**.
3. Enter the password in the **New Password** field.
4. Re-enter the password in the **Confirm Password** field.
5. Click the **Set** button, and then a new entry will be added in the table.
6. Click the **Apply** button to apply your settings.

Click the **Refresh** button to refresh this page immediately.

4.8.3 Storage Sharing

Choose menu "**USB Settings**" → "**Storage Sharing**", you can configure a USB disk drive attached to the Modem Router and view volume and share properties on this page as shown below.

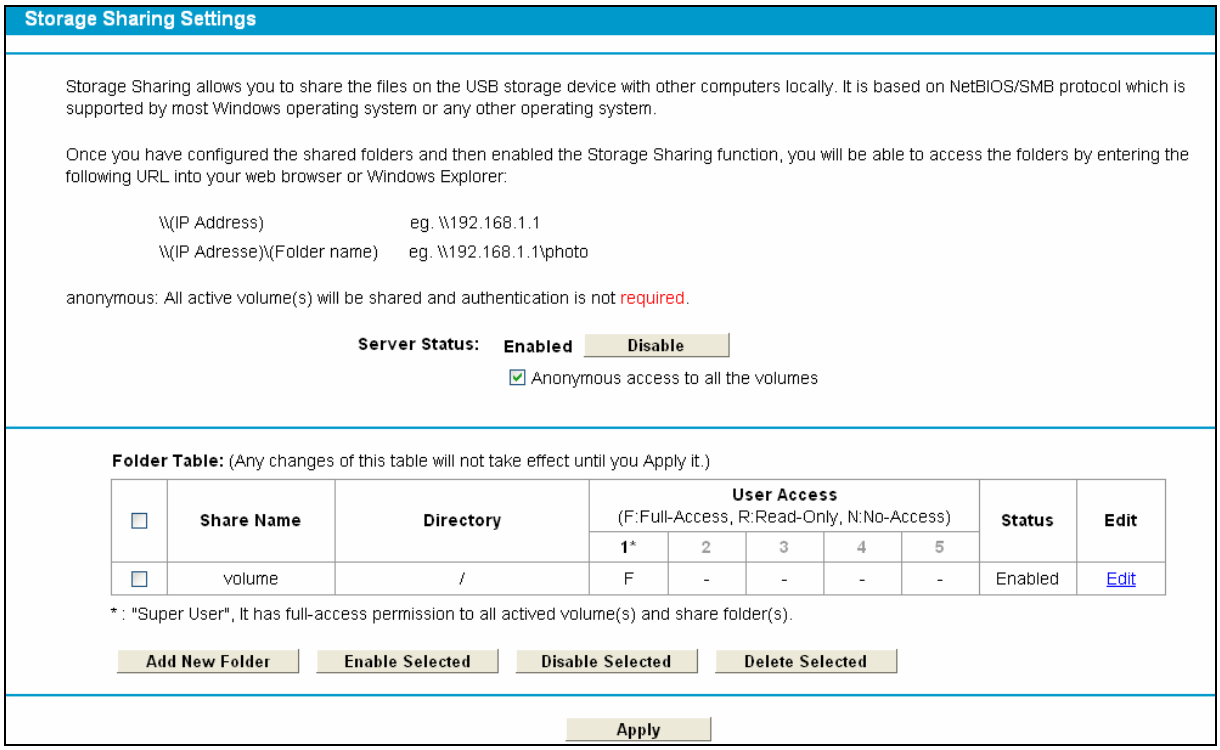

Storage Sharing Settings
Storage Sharing allows you to share the files on the USB storage device with other computers locally. It is based on NetBIOS/SMB protocol which is supported by most Windows operating system or any other operating system.
Once you have configured the shared folders and then enabled the Storage Sharing function, you will be able to access the folders by entering the following URL into your web browser or Windows Explorer:
\\(IP Address) eg. \\192.168.1.1
\\(IP Adresse)\(Folder name) eg. \\192.168.1.1\photo
anonymous: All active volume(s) will be shared and authentication is not required.
Server Status: Enabled Disable
Anonymous access to all the volumes
Folder Table: (Any changes of this table will not take effect until you Apply it.)
Share Name
Directory
User Access
(F:Full-Access, R:Read-Only, N:No-Access)
1* 2 3 4 5
Status
Edit
volume / F - - - - Enabled Edit
* : "Super User", It has full-access permission to all actived volume(s) and share folder(s).
Add New Folder
Enable Selected
Disable Selected
Delete Selected
Apply

Figure 4-58

- **Server Status:** Indicates the Storage Sharing's current status.
- **Anonymous access to all the volumes:** If this function is enabled, users can access all activated volumes of Storage Sharing without accounts.
- **Share Name:** This folder's display name.
- **Directory:** The real full path of the specified folder.
- **User Access:** The authorization of the user is displayed. * users mean Super Users who have the full-access permission to all activated volumes and share folders. Grey users mean the users who have no right to use this function. Others are common users.
- **Status:** The status of the entry is enabled or disabled.
- **Edit:** Click **Edit** in the table, and then you can modify the entry.

To add a new folder, follow the instructions below.

1. Click **Add New Folder** in Figure 4-58.

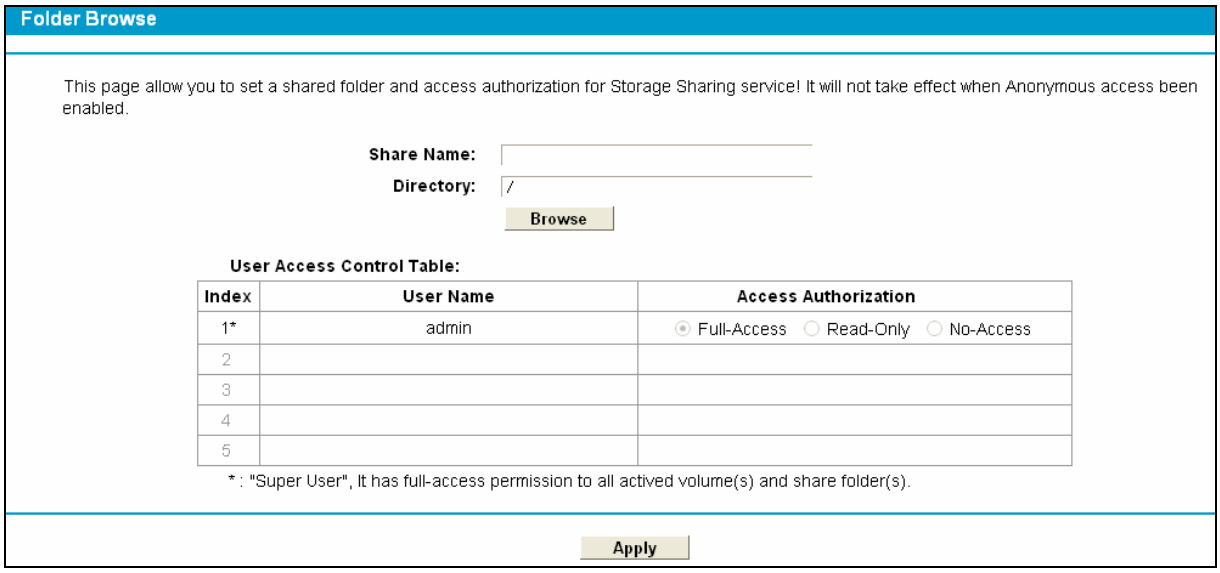


Figure 4-59

2. Click the **Browse** button, and then select the **Select Volume** from the drop-down list.
3. Enter display name of the share folder in **Share Name** filed.
4. Click the **Apply** button to apply the settings.

You can click the **upper** button to go to the upper folder

Click the **Enable/Disable Selected** button to enable or disable the selected entries.

Click the **Delete Selected** button to delete the selected entries.

☞ **Note:**

1. The max share folders number is 10. If you want to share a new folder when the number has reached 10, you can delete an existing share folder and then add a new one.
2. If you want to change the Storage Sharing settings, you can click the Apply button to make the changes take effect.

4.8.4 FTP Server

Choose menu "**USB Settings**"→"**FTP Server**", you can create an FTP server that can be accessed from the Internet or your local network.

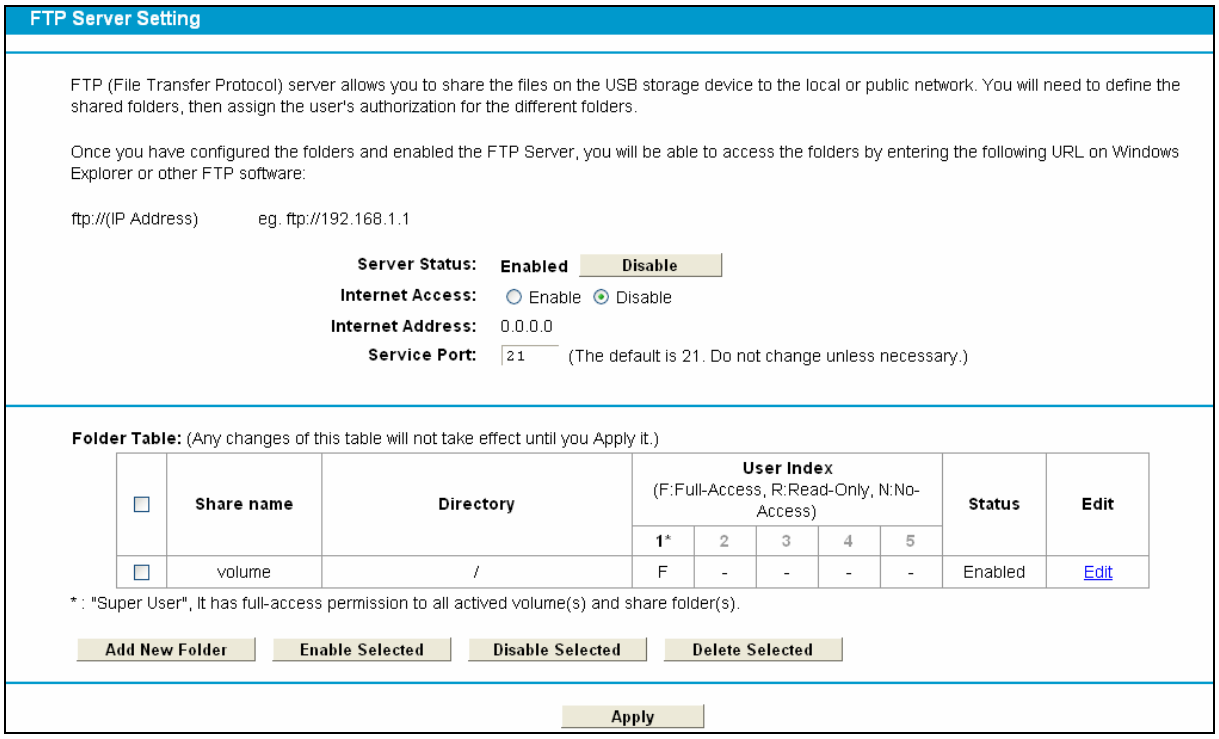

FTP Server Setting
FTP (File Transfer Protocol) server allows you to share the files on the USB storage device to the local or public network. You will need to define the shared folders, then assign the user's authorization for the different folders.
Once you have configured the folders and enabled the FTP Server, you will be able to access the folders by entering the following URL on Windows Explorer or other FTP software:
ftp://(IP Address) eg. ftp://192.168.1.1
Server Status: Enabled Disable
Internet Access: Enable Disable
Internet Address: 0.0.0.0
Service Port: 21 (The default is 21. Do not change unless necessary.)
Folder Table: (Any changes of this table will not take effect until you Apply it.)
Share name
Directory
User Index (F:Full-Access, R:Read-Only, N:No-Access)
1* 2 3 4 5
Status
Edit
volume / F - - - - Enabled Edit
* : "Super User", It has full-access permission to all actived volume(s) and share folder(s).
Add New Folder
Enable Selected
Disable Selected
Delete Selected
Apply

Figure 4-60

- **Server Status:** Indicates the FTP Server's current status.
- **Internet Access:** Enable or disable this function.
- **Internet Address:** If **Internet Access** is enabled, WAN IP will be displayed here.
- **Service Port:** Enter the FTP Port number to use. The default is 21.
- **Share Name:** This folder's display name.
- **Directory:** The real full path of the specified folder.
- **User Index:** The authorization of the user is displayed.
- **Status:** The status of the entry is enabled or disabled.
- **Edit:** Click **Edit** in the table, and then you can modify the entry.

To add a new folder, follow the instructions below.

1. Click **Add New Folder** in Figure 4-74.

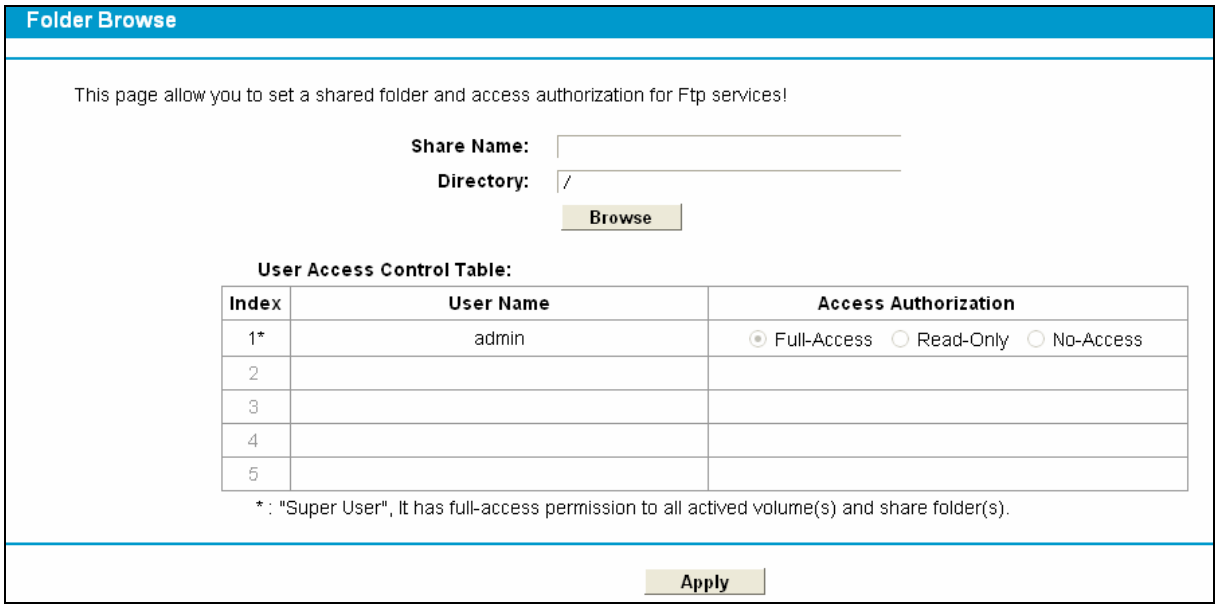


Figure 4-61

2. Click the **Browse** button, and then select the **Select Volume** from the drop-down list.
3. Enter display name of the share folder in **Share Name** filed.
4. Click the **Apply** button to apply the settings.

You can click the **upper** button to go to the upper folder.

Click the **Enable/Disable Selected** button to enable or disable the selected entries.

Click the **Delete Selected** button to delete the selected entries.

Note:

1. The max share folders number is 10. If you want to share a new folder when the number has reached 10, you can delete an existing share folder and then add a new one.
2. If you want to change the FTP settings, you can click the Apply button to make the changes take effect.

4.8.5 Media Server

Choose menu "**USB Settings**"→"**Media Server**", you can create media server that allows you to share stored content with other computers and devices on your home network and on the Internet.

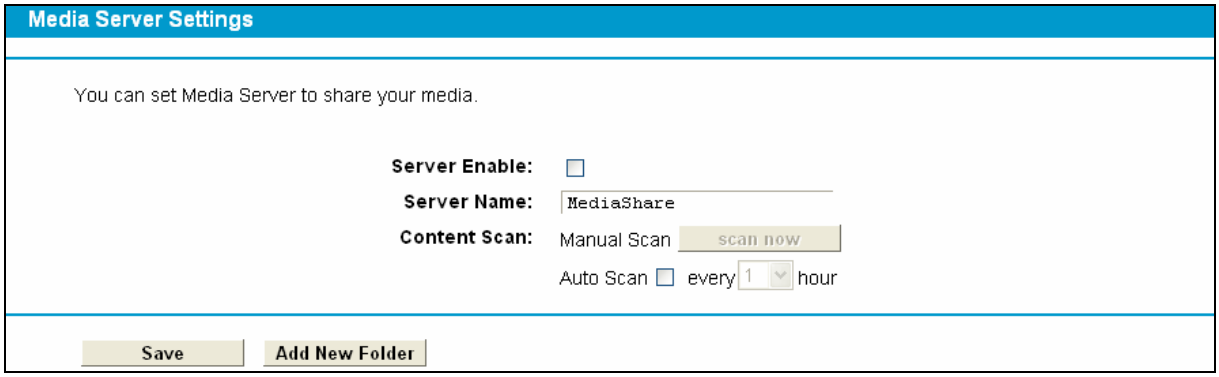


Figure 4-62

- **Server Enable:** Select this box to enable this function.
- **Server Name:** The name of this Media Server.

To add a new share folder for your media server, please follow the instructions below:

a) Click **Add Content** button, and you will see the screen as shown in Figure 4-77.

b) Enter the name of the share folder in **Share Name** field.

c) Click the **Apply** button to apply the configuration.

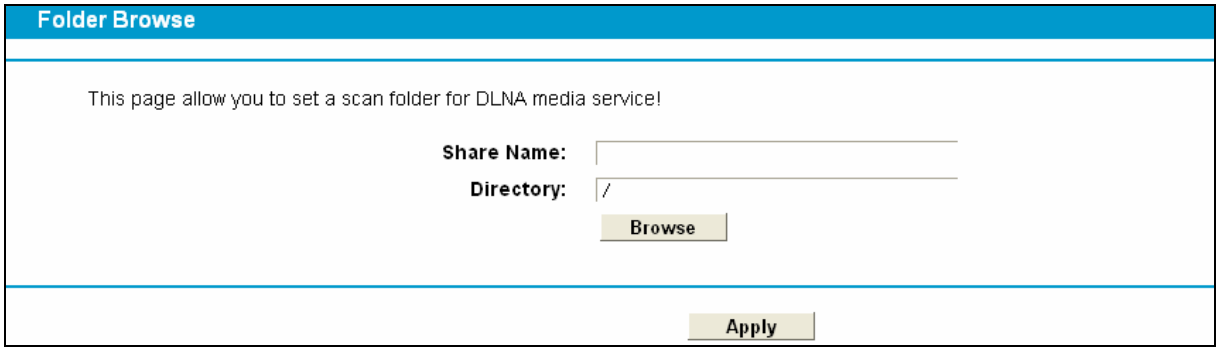


Figure 4-63

b) Click the **Scan now** to scan all the share folders immediately. You can also select the **Auto-scan**, at same time, select an auto scan interval time by drop-down list. In this case, the media server will auto scan the share folders.

Note:

The max share folders number is 6. If you want share a new folder when the numbers has been reached to be 6, you can delete a share folder and then add a new one.

4.8.6 Print Server

Choose menu "**USB Settings**"→"**Print Server**", you can configure print server on this page as shown below.

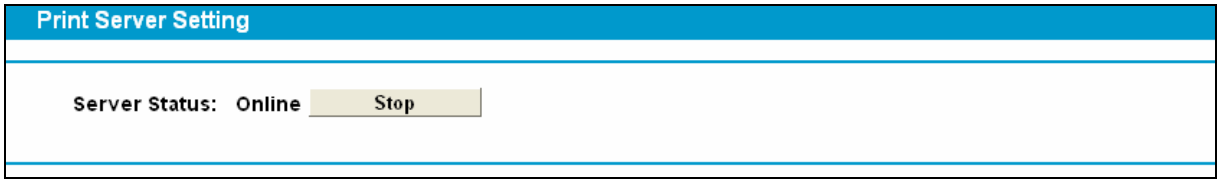


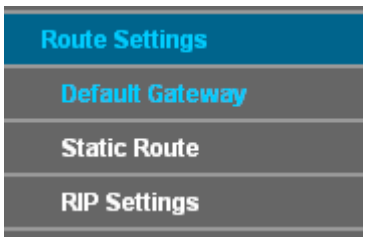
Figure 4-64

There are three states of the print server, they are as follows:

- **Online:** Indicates the print service has been turned on, and no user is using the print services at present. You can click the "**Stop**" button to stop the print service.
- **Offline:** Indicates the print service feature is disabled. You can click "**Start**" button to start the print service.
- **Busy:** Indicates the print service has been turned on, but at this moment other users are using print services.

4.9 Route Settings

Choose "**Route Settings**", it includes three menus**: Default Gateway**, **Static Route and RIP Settings**. The detailed descriptions are provided below.



4.9.1 Default Gateway

Choose "**Route Settings**"→"**Default Gateway**", you can see the Default Gateway screen. You can select a WAN Interface from the drop-down list as the system default gateway.

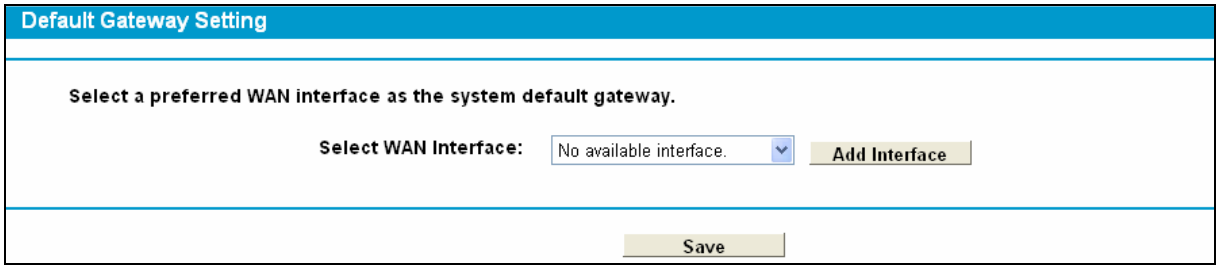


Figure 4-65

Click the **Add Interface** button, you can add WAN Interfaces.

Click the **Save** button to save your settings.

4.9.2 Static Route

Choose "**Route Settings**"→ "**Static Route**". You can see the Static Route screen, this screen allows you to configure the static routes (shown in Figure 4-66). A static route is a pre-determined path that network information must travel to reach a specific host or network.

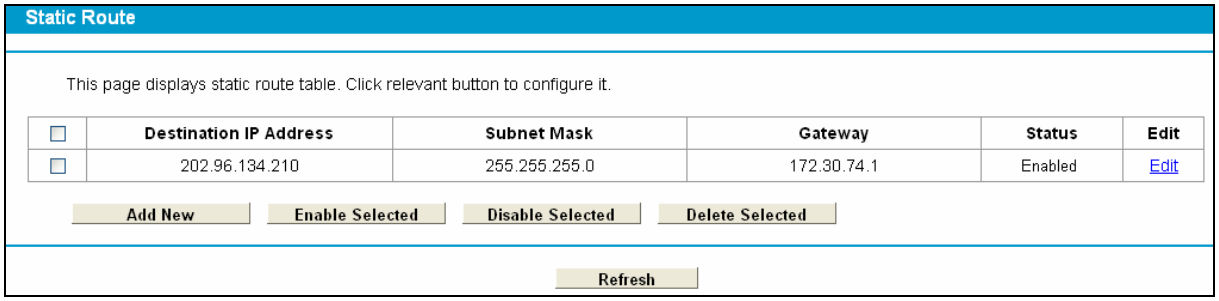


Figure 4-66

To add static routing entries:

1. Click the **Add New** button in Figure 4-66, and you will see the screen as shown in Figure 4-67.

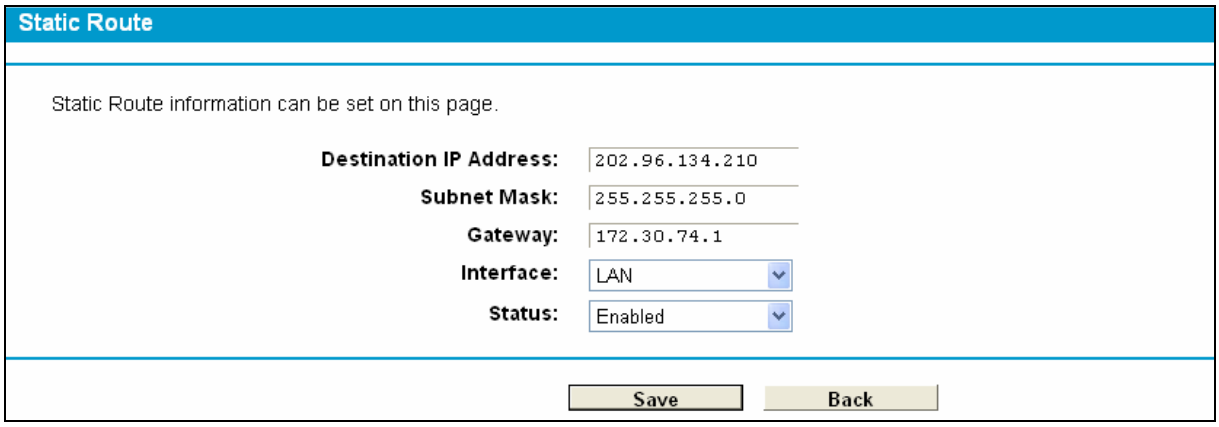


Figure 4-67

2. Enter the following data:

- **Destination IP Address:** The **Destination IP Address** is the address of the network or host that you want to assign to a static route.
- **Subnet Mask:** The **Subnet Mask** determines which portion of an IP Address is the network portion, and which portion is the host portion.
- **Gateway:** Here you should type the Gateway address correctly, and the option for **Interface** will adopt the default Gateway address for the Static Route.
- **Interface:** Select the Interface name in the text box, or else, the default Use Interface will be adopted for the Static Route.
- **Status:** Select **Enabled** or **disabled** from the drop-down list**.**

3. Click **Save** to save your settings as shown in Figure 4-67.

To modify or delete an existing entry:

1. Find the desired entry in the table.
2. Click **Edit** as desired on the **Edit** column.

Click the **Enable/ Disabled Selected** button to make selected entries enabled/ disabled.

Click the **Delete Selected** button to delete selected entries.

4.9.3 RIP Settings

Choose "**Route Settings**"→"**RIP Settings**", you can see the RIP (Routing Information Protocol) screen which allows you to configure the RIP.

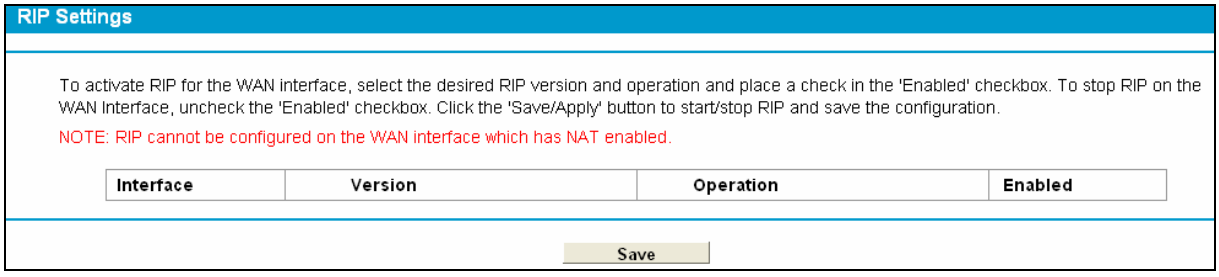
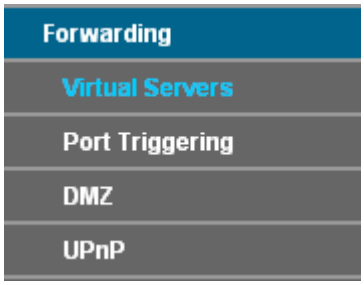

RIP Settings
To activate RIP for the WAN interface, select the desired RIP version and operation and place a check in the 'Enabled' checkbox. To stop RIP on the WAN Interface, uncheck the 'Enabled' checkbox. Click the 'Save/Apply' button to start/stop RIP and save the configuration.
NOTE: RIP cannot be configured on the WAN interface which has NAT enabled.
Interface
Version
Operation
Enabled
Save

Figure 4-68

Note:

RIP cannot be configured on the WAN Interface which has NAT enabled (such as PPPoE).

4.10 Forwarding



There are four submenus under the Forwarding menu: **Virtual Servers**, **Port Triggering**, **DMZ** and **UPnP**. Click any of them, and you will be able to configure the corresponding function.

4.10.1 Virtual Servers

Choose menu "**Forwarding**" → "**Virtual Servers**", and then you can view and add virtual servers in the next screen (shown in Figure 4-69). Virtual servers can be used for setting up public services on your LAN. A virtual server is defined as a service port, and all requests from Internet to this service port will be redirected to the computer specified by the server IP. Any PC that was used for a virtual server must have a static or reserved IP address because its IP address may change when using the DHCP function.

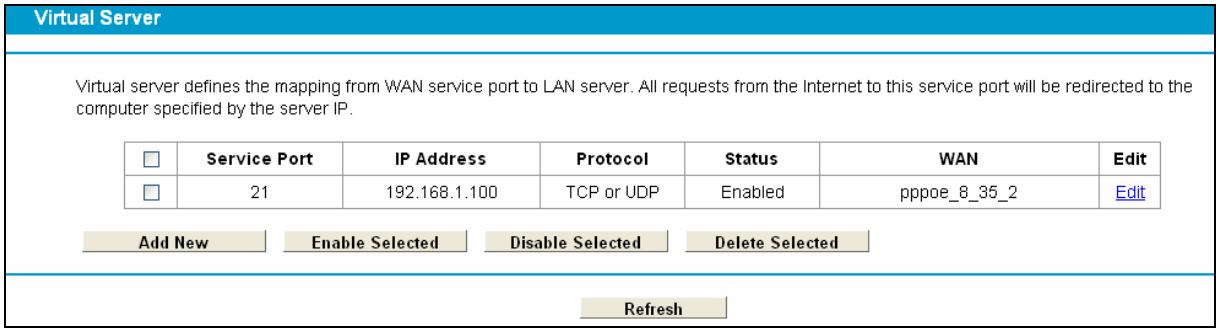


Figure 4-69

- **Service Port:** The numbers of External Service Ports. You can enter a service port or a range of service ports (the format is XXX – YYY; XXX is the Start port and YYY is the End port).
- **IP Address:** The IP address of the PC running the service application.
- **Protocol:** The protocol used for this application, either **TCP**, **UDP**, or **All** (all protocols supported by the Modem Router).
- **Status:** The status of this entry, "Enabled" means the virtual server entry is enabled.
- **Edit:** To modify or delete an existing entry.

To setup a virtual server entry:

1. Click the **Add New** button. (pop-up Figure 4-70)
2. Select the service you want to use from the **Common Service Port** list. If the **Common**

Service Port menu does not list the service that you want to use, enter the number of the service port or service port range in the **Service Port** field.

3. Select the service you want to use from the **Use Interface** list.
4. Enter the IP address of the computer running the service application in the **IP Address** field.
5. Select the protocol used for this application in the **Protocol** drop-down list, either **TCP**, **UDP**, or **All**.
6. Select the **Enabled** option in the **Status** drop-down list.

Click the **Save** button.

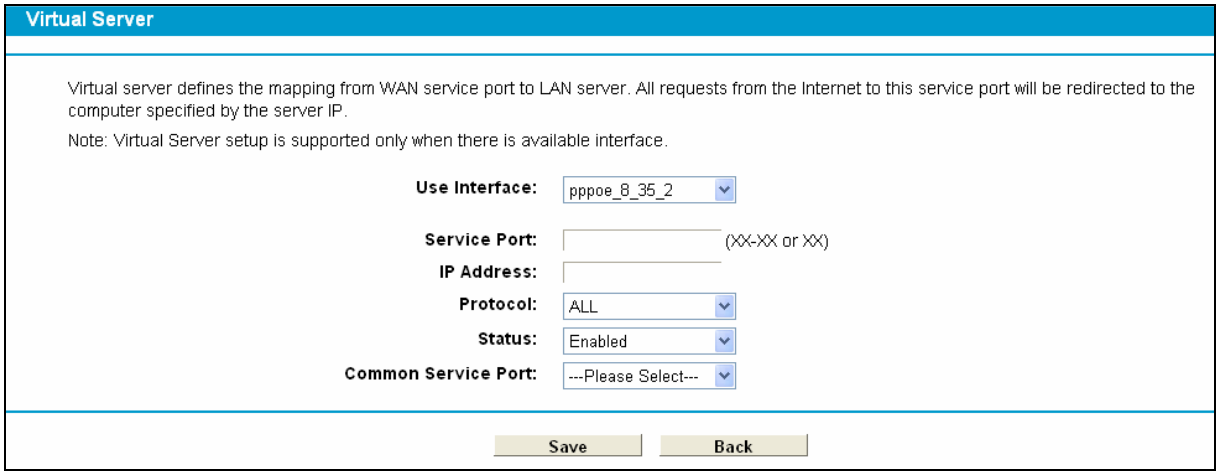

Virtual Server
Virtual server defines the mapping from WAN service port to LAN server. All requests from the Internet to this service port will be redirected to the computer specified by the server IP.
Note: Virtual Server setup is supported only when there is available interface.
Use Interface:
pppoe_8_35_2
Service Port:
(XX-XX or XX)
IP Address:
Protocol:
ALL
Status:
Enabled
Common Service Port:
---Please Select---
Save
Back

Figure 4-70

Note:

It is possible that you have a computer or server that has more than one type of available service. If so, select another service, and type the same IP address for that computer or server.

To modify or delete an existing entry:

1. Find the desired entry in the table.
2. Click **Edit** as desired on the **Edit** column.

Click the **Enable/ Disabled Selected** button to make selected entries enabled/ disabled.

Click the **Delete Selected** button to delete selected entries.

Note:

If you set the service port of the virtual server as 80, you must set the Web management port on **System Tools –> Remote Management** page to be any other value except 80 such as 8080. Otherwise there will be a conflict to disable the virtual server.

4.10.2 Port Triggering

Choose menu "**Forwarding**"→"**Port Triggering**", you can view and add port triggering in the next screen (shown in Figure 4-71). Some applications require multiple connections, like Internet games, video conferencing, Internet telephoning and so on. Port Triggering is used for some of these applications that cannot work with a pure NAT Modem Router.

Figure 4-71

To add a new rule, follow the steps below.

1. Click the **Add New** button, the next screen will pop-up as shown in Figure 4-72.
2. Select a common application from the **Common Service Port** drop-down list, then the **Trigger Port** field and the **Open Ports** field will be automatically filled. If the **Common Service Port** do not have the application you need, enter the **Trigger Port** and the **Open Ports** manually.
3. Select the protocol used for Trigger Port from the **Trigger Protocol** drop-down list, either **TCP**, **UDP**, or **All**.
4. Select the protocol used for Incoming Ports from the **Incoming Protocol** drop-down list, either **TCP** or **UDP**, or **All.**
5. Select **Enable** in **Status** field.
6. Click the **Save** button to save the new rule.

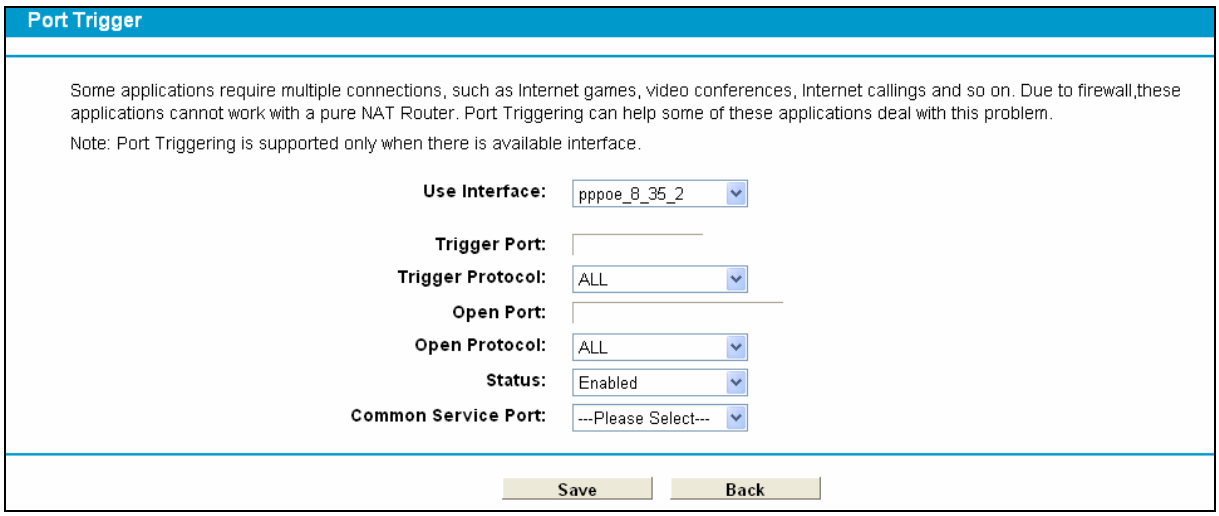

Port Trigger
Some applications require multiple connections, such as Internet games, video conferences, Internet callings and so on. Due to firewall,these applications cannot work with a pure NAT Router. Port Triggering can help some of these applications deal with this problem.
Note: Port Triggering is supported only when there is available interface.
Use Interface:
pppoe_8_35_2
Trigger Port:
Trigger Protocol:
ALL
Open Port:
Open Protocol:
ALL
Status:
Enabled
Common Service Port:
---Please Select---
Save
Back

Figure 4-72

- **Trigger Port:** The port for outgoing traffic. An outgoing connection using this port will trigger this rule.
- **Trigger Protocol:** The protocol used for Trigger Ports, either **TCP**, **UDP**, or **All** (all protocols supported by the Modem Router).
- **Open Port:** The port or port range used by the remote system when it responds to the outgoing request. A response using one of these ports will be forwarded to the PC which triggered this rule. You can input at most 5 groups of ports (or port sections). Every group of ports must be separated with ",", for example, 2000-2038, 2046, 2050-2051, 2085, 3010-3030.

- **Open Protocol:** The protocol used for **Incoming Port**, either **TCP**, **UDP**, or **ALL** (all protocols supported by the Modem Router).
- **Status:** The status of this entry, Enabled means the Port Triggering entry is enabled.
- **Modify:** To modify or delete an existing entry.
- **Common Service Port:** Some popular applications already listed in the drop-down list of **Open Protocol**.

To modify or delete an existing entry:

1. Find the desired entry in the table.
2. Click **Edit** as desired on the **Edit** column.

Click the **Enable/ Disabled Selected** button to make selected entries enabled/ disabled.

Click the **Delete Selected** button to delete selected entries.

Once the Modem Router is configured, the operation is as follows:

1. A local host makes an outgoing connection to an external host using a destination port number defined in the **Trigger Port** field.
2. The Modem Router records this connection, opens the incoming port or ports associated with this entry in the **Port Triggering** table, and associates them with the local host.
3. When necessary, the external host will be able to connect to the local host using one of the ports defined in the **Incoming Ports** field.

☞ **Note:**

1. When the trigger connection is released, the corresponding opened ports will be closed.
2. Each rule can only be used by one host on the LAN at a time. The trigger connection of other hosts on the LAN will be refused.
3. **Open Ports** ranges cannot overlap each other.

4.10.3 DMZ

Choose menu "**Forwarding→DMZ**", and then you can view and configure DMZ host in the screen (shown in Figure 4-73).The DMZ host feature allows one local host to be exposed to the Internet for a special-purpose service such as Internet gaming or videoconferencing. The Modem Router forwards packets of all services to the DMZ host. Any PC whose port is being forwarded must have its DHCP client function disabled and should have a new static IP Address assigned to it because its IP Address may be changed when using the DHCP function.

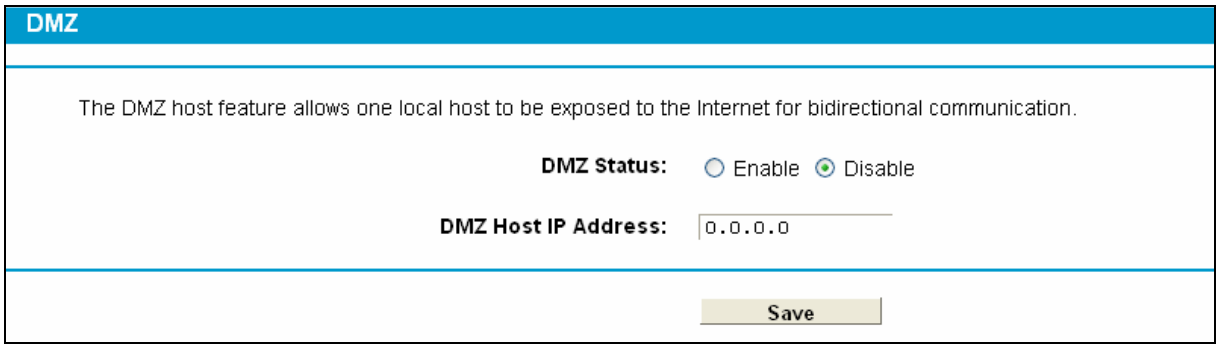


Figure 4-73

To assign a computer or server to be a DMZ server:

1. Click the **Enable** button.
2. Enter the IP address of a local PC that is set to be DMZ host in the **DMZ Host IP Address** field.
3. Click the **Save** button.

4.10.4 UPnP

Choose menu "**Forwarding→UPnP**", and then you can view the information about **UPnP** in the screen (shown in Figure 4-74). The **Universal Plug and Play (UPnP)** feature allows the devices, such as Internet computers, to access the local host resources or devices as needed. UPnP devices can be automatically discovered by the UPnP service application on the LAN.

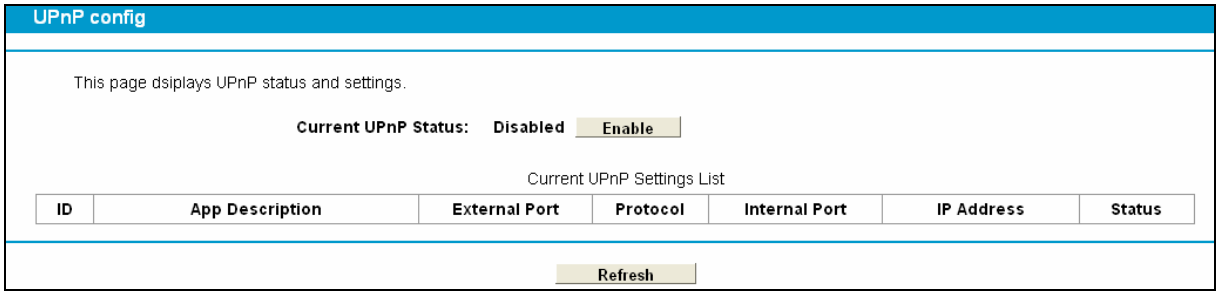


Figure 4-74

- **Current UPnP Status:** UPnP can be enabled or disabled by clicking the **Enable** or **Disable** button. This feature is enabled by default.
- **Current UPnP Settings List:** This table displays the current UPnP information.

  - **App Description:** The description about the application which initiates the UPnP request.
  - **External Port:** The port which the Modem Router opened for the application.
  - **Protocol:** The type of protocol which is opened.
  - **Internal Port:** The port which the Modem Router opened for local host.
  - **IP Address:** The IP address of the local host which initiates the UPnP request.
  - **Status:** Either Enabled or Disabled. "Enabled" means that the port is still active; otherwise, the port is inactive.

Click the **Enable** button to enable UPnP.

Click the **Disable** button to disable UPnP.

Click the **Refresh** button to update the Current UPnP Settings List.

4.11 Parental Control

Choose menu "**Parental Control**", and you can configure the parental control in the screen as shown in Figure 4-75. The Parental Control function can be used to control the internet activities of the child, limit the child to access certain websites and restrict the time of surfing.

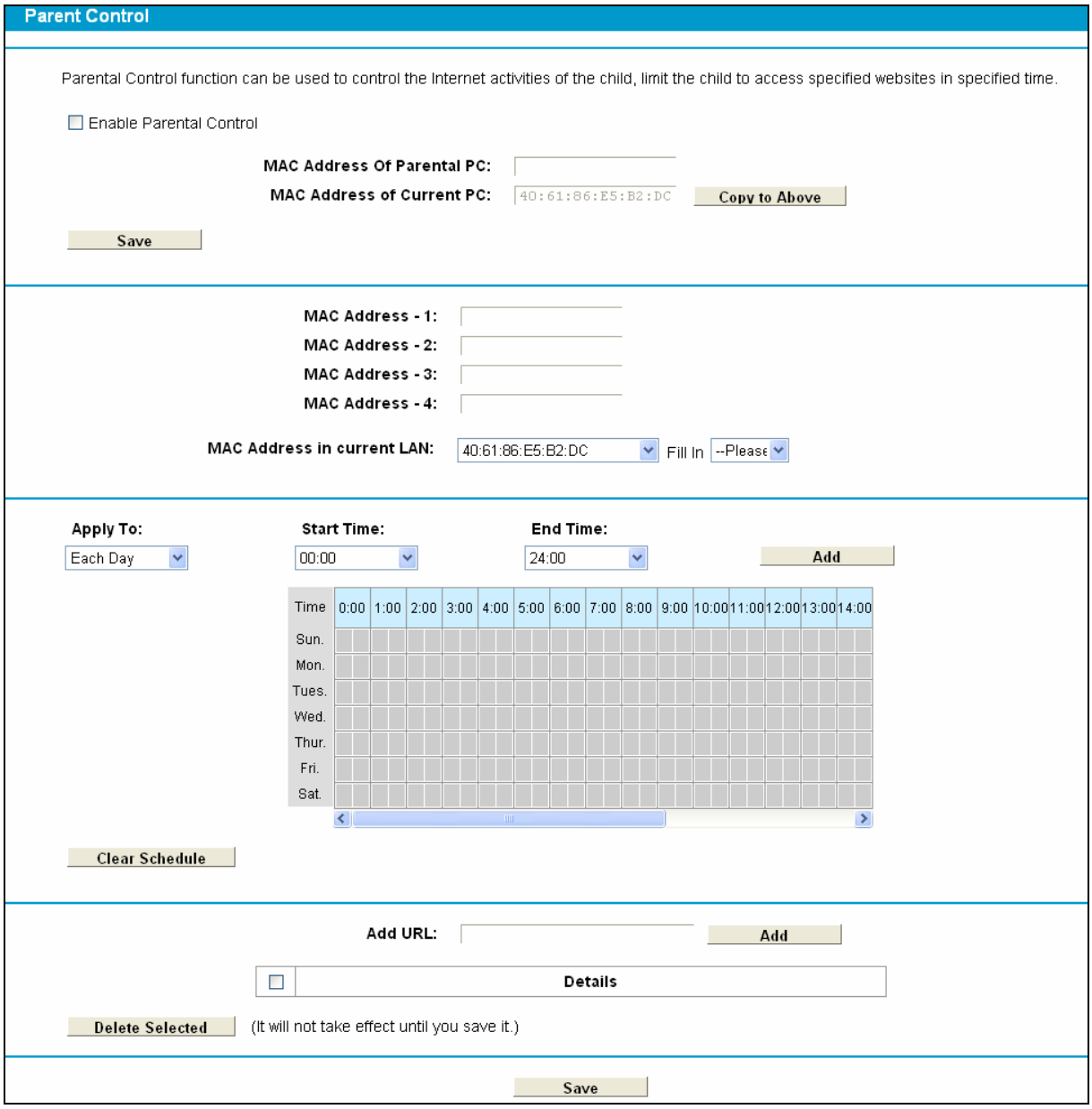


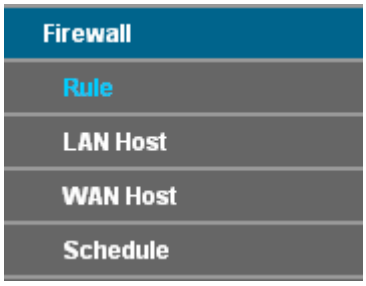
Figure 4-75

- **Enable Parental Control:** Check the box if you want this function to take effect. This function is disabled by default.
- **MAC Address of Parental PC:** In this field, enter the MAC address of the controlling PC, or you can make use of the **Copy To Above** button below.

- **MAC Address of Current PC:** This field displays the MAC address of the PC that is managing this Modem Router. If the MAC Address of your adapter is registered, you can click the Copy To Above button to fill this address to the MAC Address of Parental PC field above.
- **Add URL:** Here you can input the net addresses which the child is allowed to access.

Click the **Save** button to save your settings.

4.12 Firewall



There are four submenus under the Firewall menu: **Rule**, **LAN Host**, **WAN Host** and **Schedule**. Click any of them, and you will be able to configure the corresponding function.

4.12.1 Rule

Choose menu "**Firewall**" → "**Rule**", and then you can view and set Access Control rules in the screen as shown in Figure 4-76.

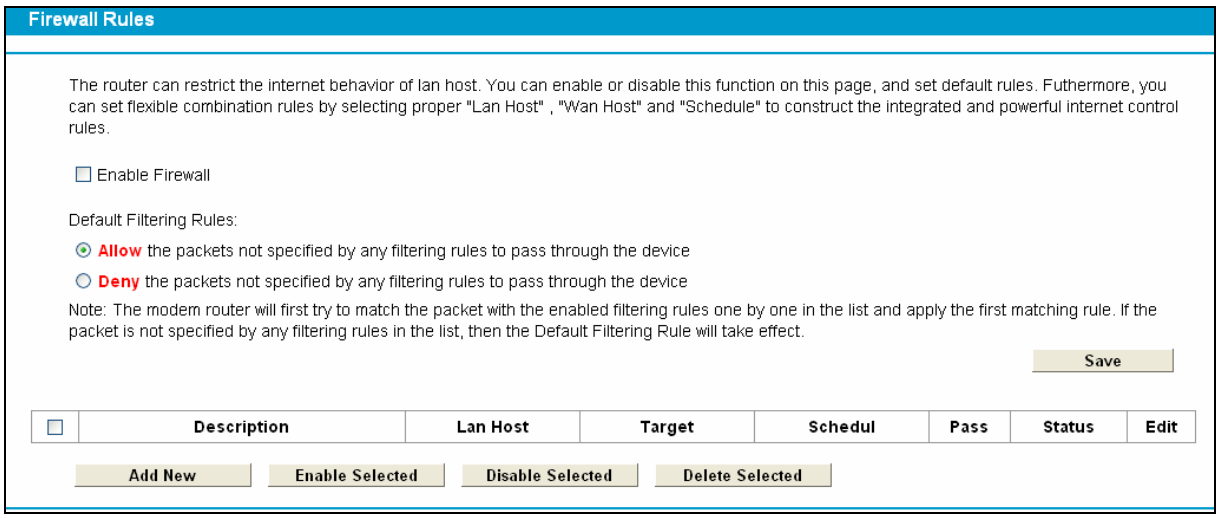

Firewall Rules
The router can restrict the internet behavior of lan host. You can enable or disable this function on this page, and set default rules. Futhermore, you can set flexible combination rules by selecting proper "Lan Host" , "Wan Host" and "Schedule" to construct the integrated and powerful internet control rules.
Enable Firewall
Default Filtering Rules:
Allow the packets not specified by any filtering rules to pass through the device
Deny the packets not specified by any filtering rules to pass through the device
Note: The modem router will first try to match the packet with the enabled filtering rules one by one in the list and apply the first matching rule. If the packet is not specified by any filtering rules in the list, then the Default Filtering Rule will take effect.
Save
Description
Lan Host
Target
Schedul
Pass
Status
Edit
Add New
Enable Selected
Disable Selected
Delete Selected

Figure 4-76

- **Enable Firewall:** Select the check box to enable the Firewalll function, so the Default Filtering Rules can take effect.
- **Description:** Here displays the description of the rule and this name is unique.
- **LAN Host:** Here displays the host selected in the corresponding rule.
- **Target:** Here displays the target selected in the corresponding rule.
- **Schedule:** Here displays the schedule selected in the corresponding rule.
- **Status:** Here displays the status of the rule, enabled or not.
- **Edit:** Here you can edit or delete an existing rule.

- **Add New:** Click the **Add New** button to add a new rule entry.
- **Enable Selected:** Click the **Enable Selected** button to enable the selected rules in the list.
- **Disable Selected:** Click the **Disable Selected** button to disable the selected rules in the list.
- **Delete Selected:** Click the **Delete Selected** button to delete the selected entries in the table.

The methods to add a new rule:

1. Click the **Add New** button and the next screen will pop up as shown in Figure 4-77.
2. Give a name (e.g. Rule_1) for the rule in the **Description** field.
3. Select a host from the **LAN Host** drop-down list or choose "**Add LAN Host**".
4. Select a target from the **WAN Host** drop-sown list or choose "**Add WAN Host**".
5. Select a schedule from the **Schedule** drop-down list or choose "**Add Schedule**".
6. In the **Action** field, select **Deny** or **Allow** to deny or allow your entry.
7. In the **Status** field, select **Enabled** or **Disabled** to enable or disable your entry.
8. In the **Direction** field, select **IN** or **OUT** from the drop-down list for the direction.
9. In the **Protocol** field, here are four options, All, TCP, UDP, and ICMP. Select one of them from the drop-down list for the target.
10. Click the **Save** button.

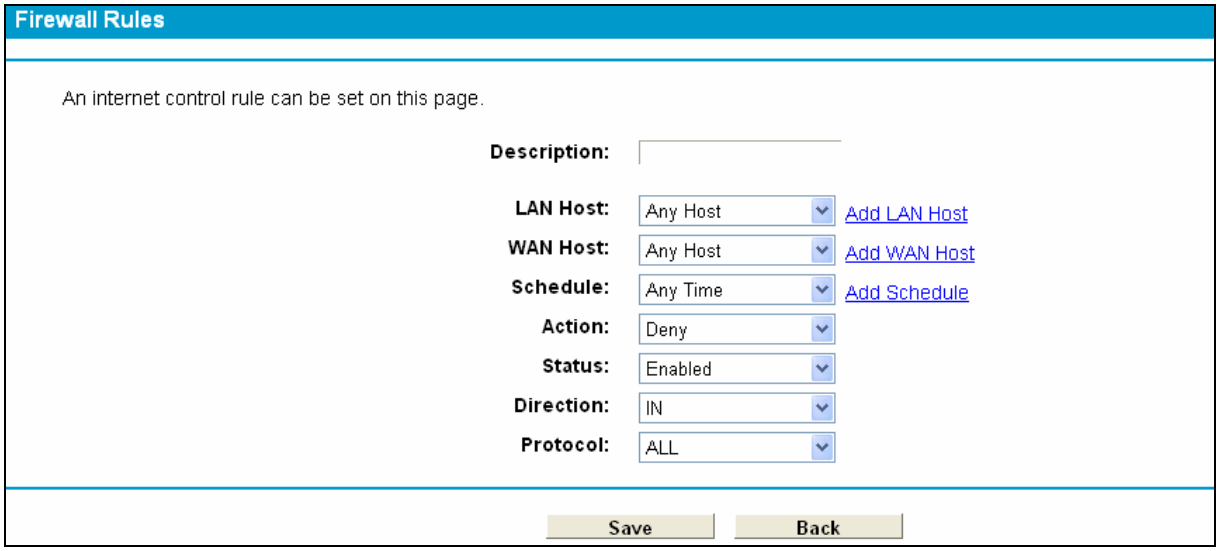


Figure 4-77

4.12.2 LAN Host

Choose menu "**Firewall**" → "**LAN Host**", and then you can view and set a Host list in the screen as shown in Figure 4-78.

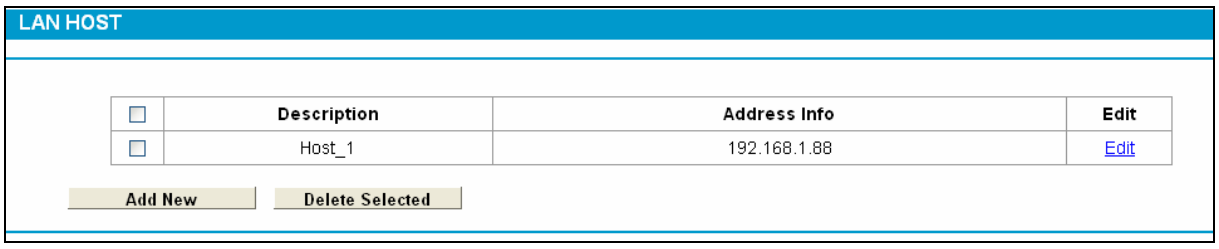


Figure 4-78

- **Description:** Here displays the description of the host and this description is unique.
- **Address Info:** Here displays the information about the host. It can be IP or MAC.
- **Edit:** To modify an existing entry.

To add a new entry, please follow the steps below.

1. Click the **Add New** button.
2. In the **Mode** field, select IP Address or MAC Address.
   - If you select IP Address, please follow the steps below:
     1) In **Description** field, create a unique description for the host (e.g. Host_1).
     2) In **IP Address** field, enter the IP address.
   - If you select MAC Address, please follow the steps below:
     1) In **Description** field, create a unique description for the host (e.g. Host_1).
     2) In **MAC Address** field, enter the MAC address.
3. Click the **Save** button to complete the settings.

Click the **Delete Selected** button to delete the selected entries in the table.

4.12.3 WAN Host

Choose menu "**Firewall**" → "**WAN Host**", and then you can view and set a Host list in the screen as shown in Figure 4-79.

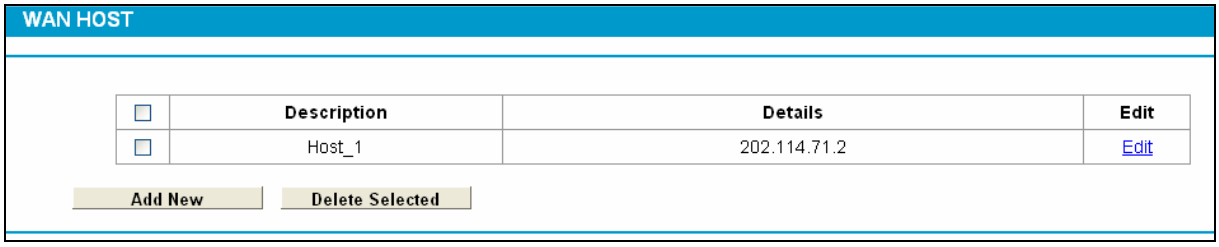


Figure 4-79

- **Description:** Here displays the description about the WAN and this description is unique.
- **Details:** The details can be IP address, port, or domain name.
- **Edit:** To modify an existing entry.

To add a new entry, please follow the steps below.

1. Click the **Add New** button.
2. In Mode field, select **IP Address**, **MAC Address** or **URL Address**.

If you select **IP Address**, the screen shown is Figure 4-80.

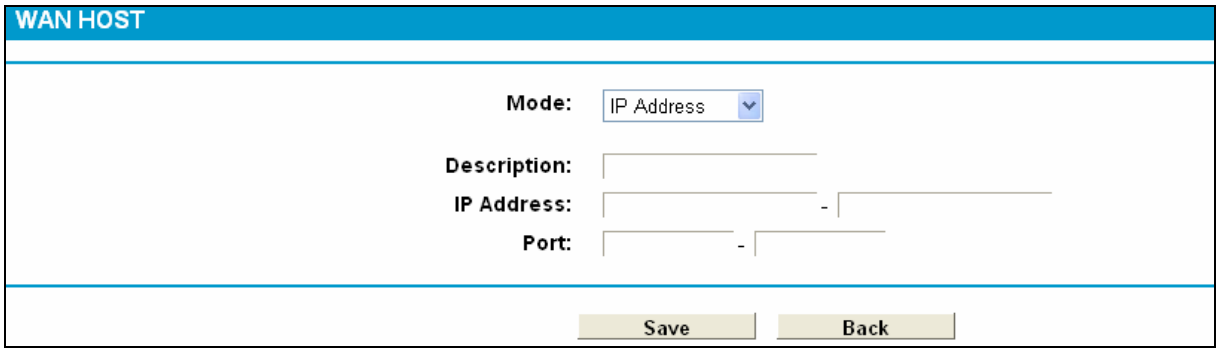


Figure 4-80

1) In **Description** field, create a unique description for the host (e.g. Host_1).

2) In **IP Address** field, enter the IP address.

If you select **MAC Address**, the screen shown is Figure 4-81.

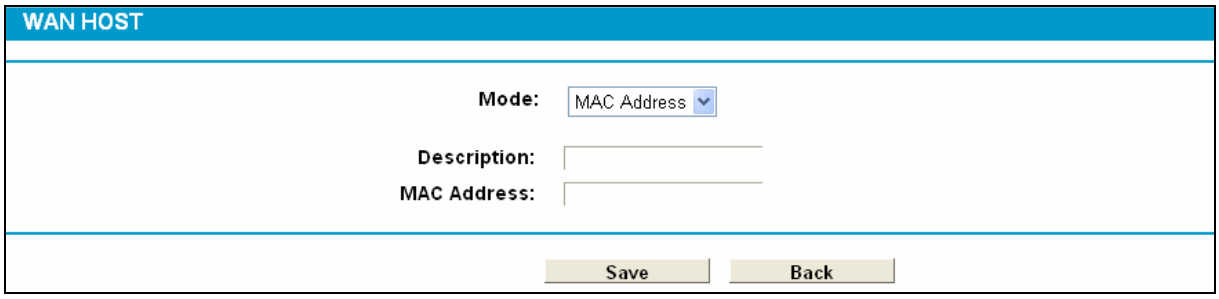


Figure 4-81

1) In **Description** field, create a unique description for the host (e.g. Host_1).

2) In **MAC Address** field, enter the MAC address.

If you select **URL Address**, the screen shown is Figure 4-82.

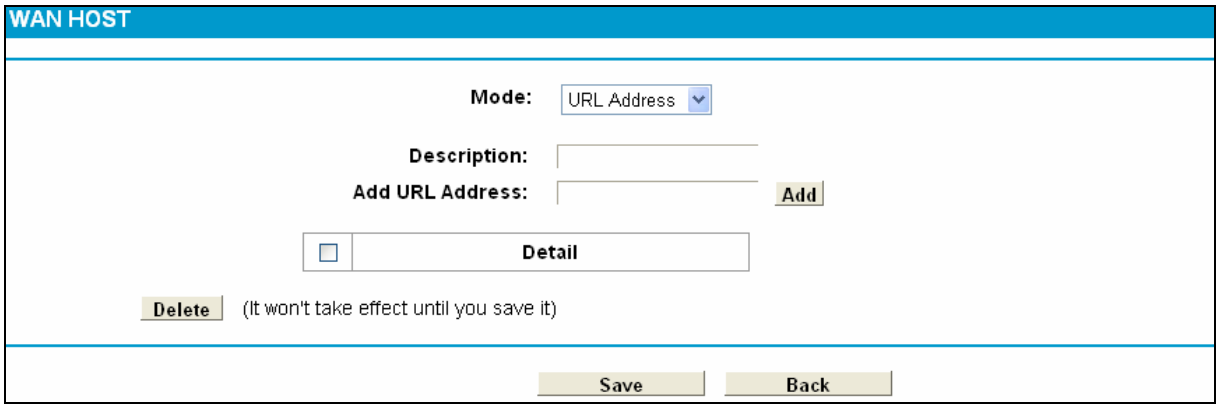


Figure 4-82

1) In **Description** field, create a unique description for the host (e.g. Host_1).

2) Enter the URL address in the **Add URL Address** field, and then click the **Add** button. The URL address will be shown in the **Detail** table. If you click the **Delete** button, the existing URL address in the **Detail** table can be deleted.

3. Click the **Save** button to complete the settings.

4.12.4 Schedule

Choose menu "**Firewall**" → "**Schedule**", and then you can view and set a Schedule list in the next screen as shown in Figure 4-83.

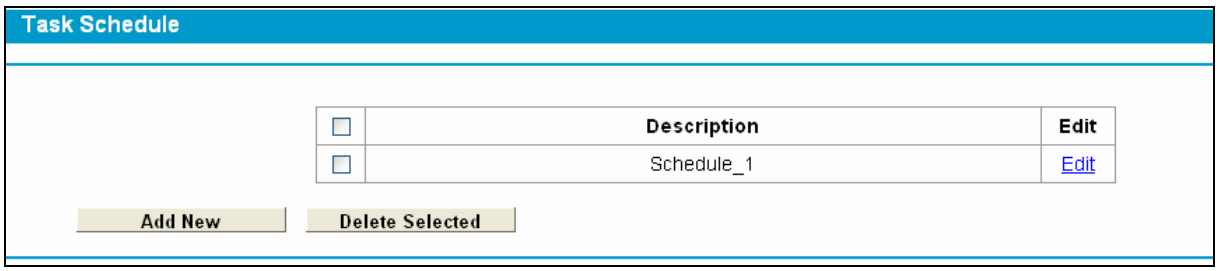


Figure 4-83

- **Description:** Here displays the description of the schedule and this description is unique.
- **Edit:** Here you can modify an existing schedule.

To add a new schedule, follow the steps below:

1. Click **Add New** button and the next screen will pop-up as shown in Figure 4-84.
2. In **Description** field, create a unique description for the schedule (e.g. Schedule_1).
3. In **Apply To** field, select the day or days you need.
4. In time field, you can select all day-24 hours or you may enter the **Start Time** and **Stop Time** in the corresponding field.
5. Click **Save** to complete the settings.

Click the **Clear Schedule** button to clear your settings in the table.

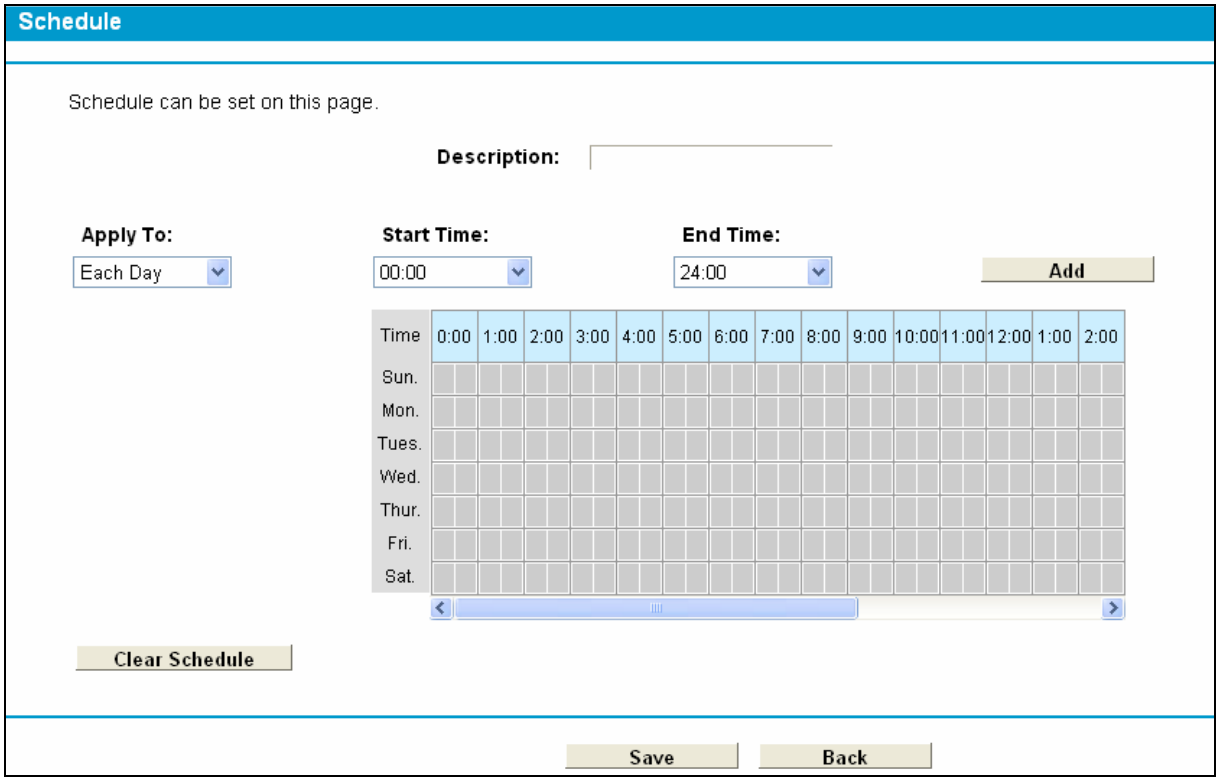
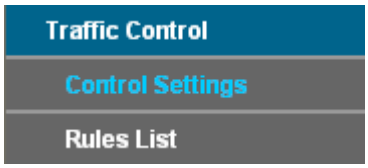


Figure 4-84

Click the **Delete Selected** button to delete the selected entries in the table.

4.13 Traffic Control



There are two submenus under the Traffic Control menu: **Control Settings** and **Rules List**. Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

4.13.1 Control Settings

Choose menu "**Traffic Control**" → "**Control Settings**", and then you can configure the Upstream Bandwidth and Downstream Bandwidth in the next screen. The values you configure should be less than 100000Kbps. For optimal control of the bandwidth, please select the right Line Type and ask your ISP for the total bandwidth of the egress and ingress.

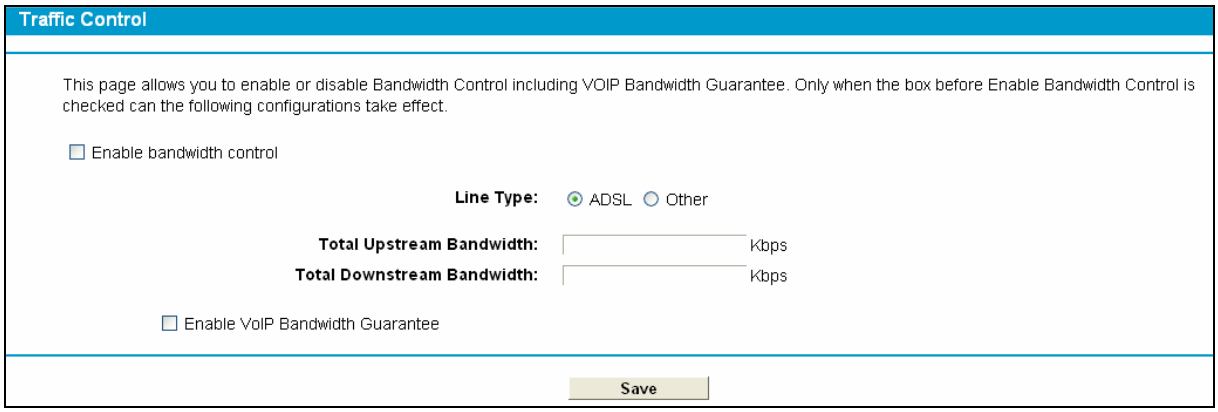

Traffic Control
This page allows you to enable or disable Bandwidth Control including VOIP Bandwidth Guarantee. Only when the box before Enable Bandwidth Control is checked can the following configurations take effect.
Enable bandwidth control
Line Type:
ADSL
Other
Total Upstream Bandwidth:
Kbps
Total Downstream Bandwidth:
Kbps
Enable VoIP Bandwidth Guarantee
Save

Figure 4-85

- **Enable Bandwidth Control:** Check this box so that the Bandwidth Control settings can take effect.
- **Line Type:** Select the right type for you network connection. If you don't know how to choose, please ask your ISP for the information.
- **Total Upstream Bandwidth** - The upload speed through the WAN port.
- **Total Downstream Bandwidth -** The download speed through the WAN port.

4.13.2 Rules List

Choose menu "**Traffic Control**" → "**Rules List**", and then you can view and configure the Bandwidth Control rules in the screen below.

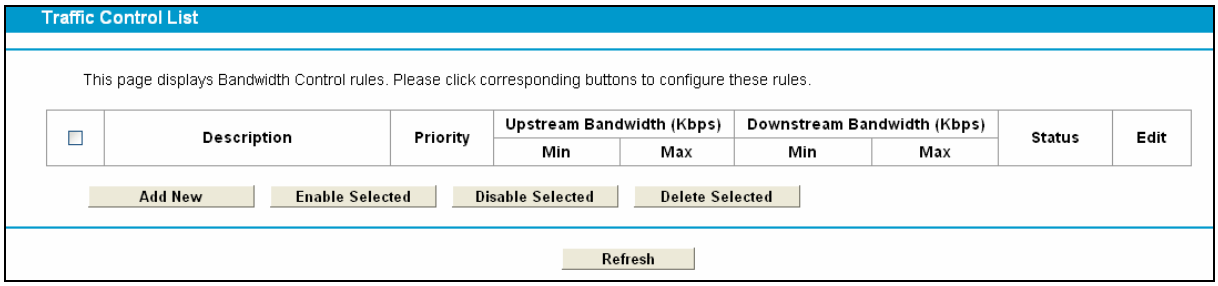


Figure 4-86

- **Description:** This is the information about the rules such as address range.
- **Upstream Bandwidth:** This field displays the max and mix upload bandwidth through the WAN port, the default is 0.
- **Downstream Bandwidth:** This field displays the max and mix download bandwidth through the WAN port, the default is 0.
- **Edit:** Click **Edit** to modify the rule.

To add/modify a Bandwidth Control rule, follow the steps below.

1. Click **Add New** shown in Figure 4-86, you will see a new screen shown in Figure 4-87.
2. Enter the information like the screen shown below.

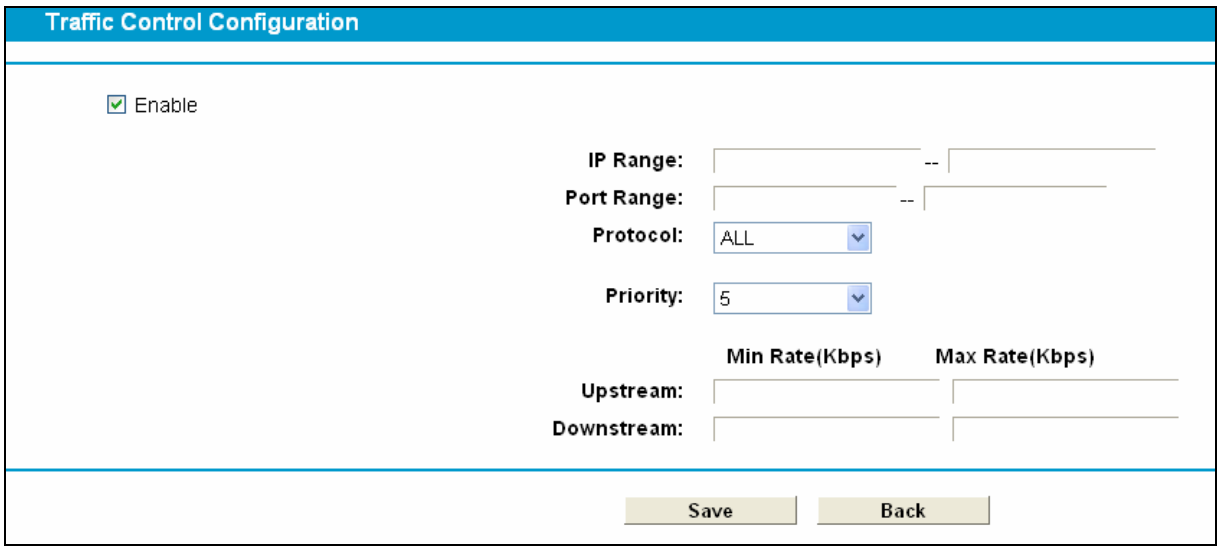
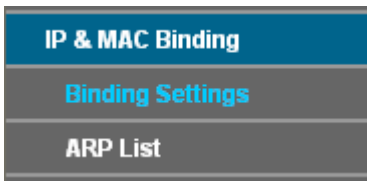


Figure 4-87

3. Click the **Save** button.

4.14 IP&MAC Binding



There are two submenus under the IP &MAC Binding menu: **Binding Settings** and **ARP List**. Click any of them, and you will be able to scan or configure the corresponding function. The detailed explanations for each submenu are provided below.

4.14.1 Binding Settings

This page displays the **IP & MAC Binding Setting** table; you can operate it in accord with your desire (shown in Figure 4-88).

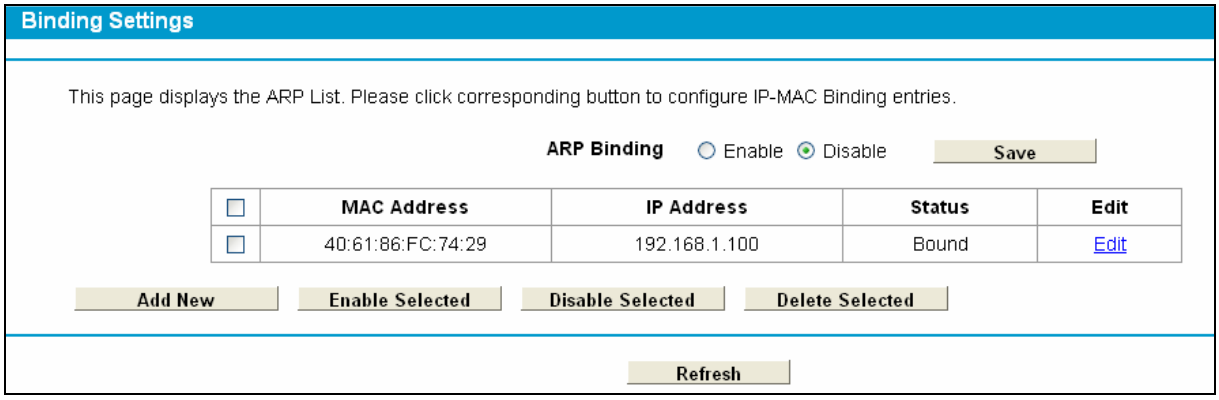


Figure 4-88

- **MAC Address:** The MAC address of the controlled computer in the LAN.
- **IP Address:** The assigned IP address of the controlled computer in the LAN.
- **Bound:** Check this option to enable ARP binding for a specific device.
- **Edit:** To modify or delete an existing entry.

When you want to add or modify an IP & MAC Binding entry, you can click the **Add New** button or **Edit** button, and then you will go to the next page. This page is used for adding or modifying an IP & MAC Binding entry (shown in Figure 4-89).

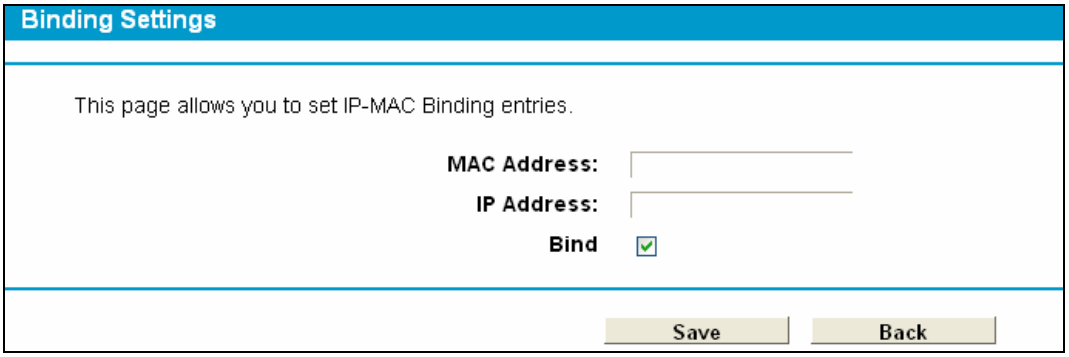


Figure 4-89

To add IP & MAC Binding entries, follow the steps below.

1. Click the **Add New** button as shown in Figure 4-88.
2. Enter the MAC Address and IP Address.
3. Select the Bind checkbox.
4. Click the **Save** button to save it.

To modify or delete an existing entry, follow the steps below.

1. Find the desired entry in the table.
2. Click **Edit** as desired on the **Edit** column.

Click the **Enable/ Disable Selected** button to make selected entries enabled or disabled.

Click the **Delete Selected** button to delete selected entries.

4.14.2 ARP List

To manage the computer, you could observe the computers in the LAN by checking the relationship of MAC address and IP address on the ARP list, and you could also configure the items on the ARP list. This page displays the ARP List; it shows all the existing IP & MAC Binding entries (shown in Figure 4-90).

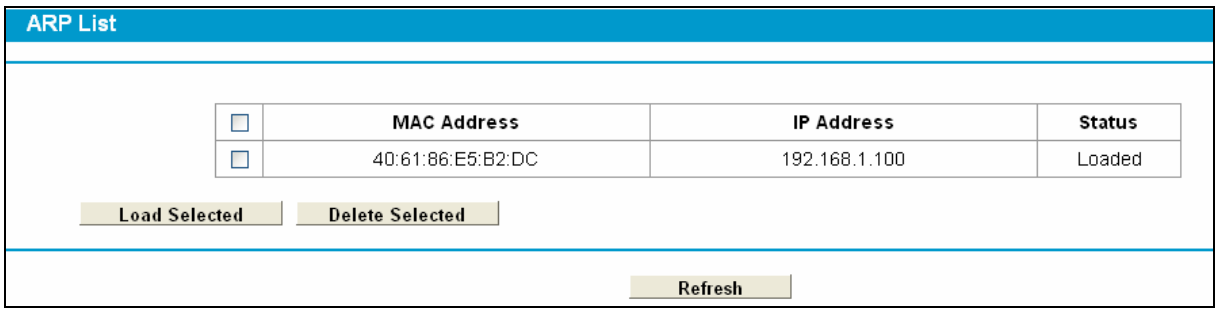


Figure 4-90

- **MAC Address:** The MAC address of the controlled computer in the LAN.
- **IP Address:** The assigned IP address of the controlled computer in the LAN.
- **Status:** Indicates whether or not the MAC and IP addresses are bound.
- **Load:** Load the item to the IP & MAC Binding list.

Click the **Load Selected** button to load selected items to the IP & MAC Binding list.

Click the **Refresh** button to refresh all items.

4.15 Dynamic DNS

Choose menu "**Dynamic DNS**", and you can configure the Dynamic DNS function.

The Modem Router offers the **DDNS** (Dynamic Domain Name System) feature, which allows the hosting of a website, FTP server, or e-mail server with a fixed domain name (named by yourself) and a dynamic IP address, and then your friends can connect to your server by entering your domain name no matter what your IP address is. Before using this feature, you need to sign up for DDNS service providers such as www.dyndns.org. The Dynamic DNS client service provider will give you a password or key.

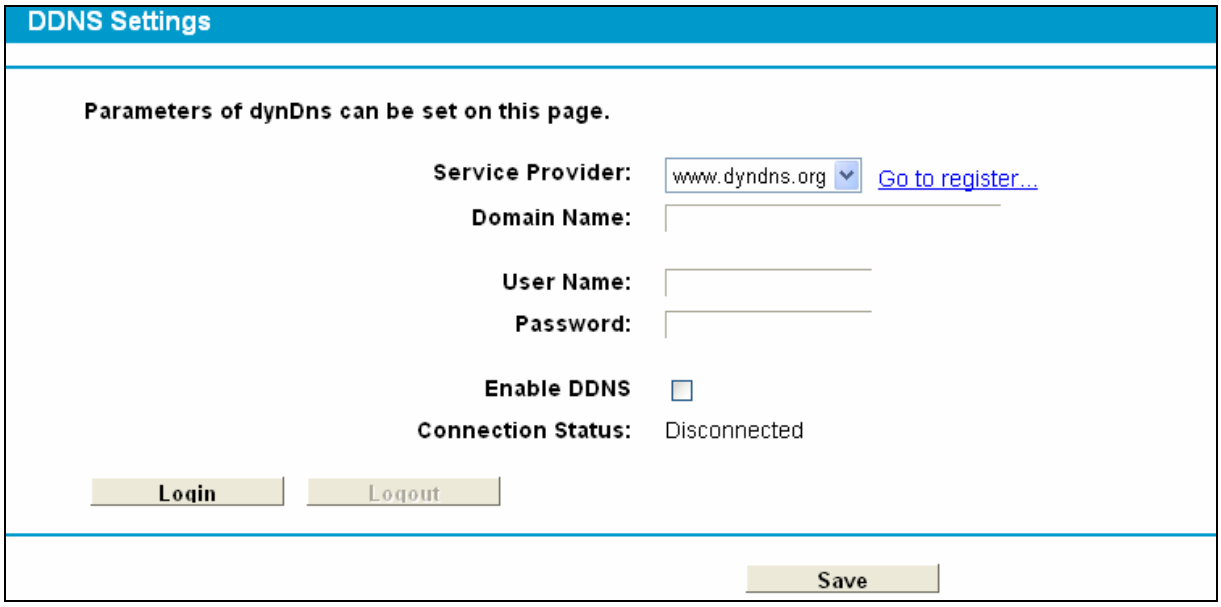


Figure 4-91

- **Service Provider:** This field displays the service provider of DDNS.
- **Domain Name:** Enter the Domain name you received from dynamic DNS service provider.
- **Username & Password:** Type the “User Name” and “Password” for your DDNS account.
- **Enable DDNS:** Activate the DDNS function or not.
- **Login/ Logout:** Login to or logout of the DDNS service.

4.16 Diagnostic

Choose “**Diagnostic**”, you can view the test results for the connectivity of the physical layer and protocol layer for both LAN and WAN sides in the screen. Select the desired type and click the start button.

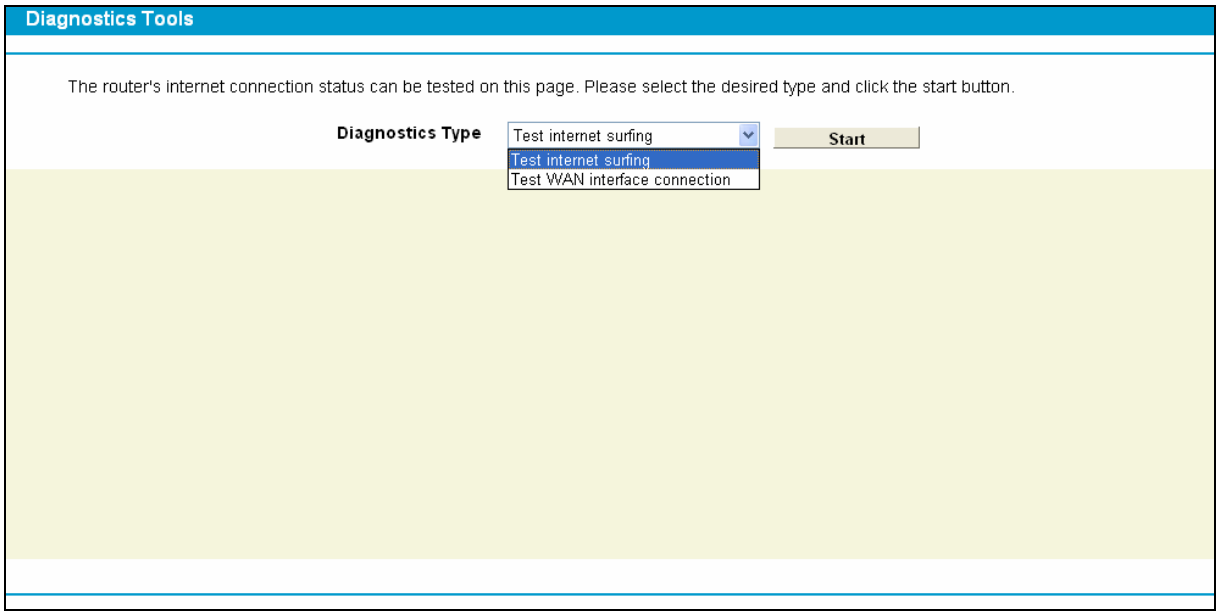

Diagnostics Tools
The router's internet connection status can be tested on this page. Please select the desired type and click the start button.
Diagnostics Type
Test internet surfing
Start
Test internet surfing
Test WAN interface connection

Figure 4-92

4.17 System Tools

Choose menu "**System Tools**", and you can see the submenus under the main menu: **System Log**, **Time Settings**, **Manage Control**, **CWMP Settings**, **SNMP Settings**, **Backup & Restore**, **Factory Defaults**, **Firmware Upgrade**, **Reboot** and **Statistics.** Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

4.17.1 System Log

Choose menu "**System Tools**" → "**System Log**", and then you can view the logs of the Modem Router.

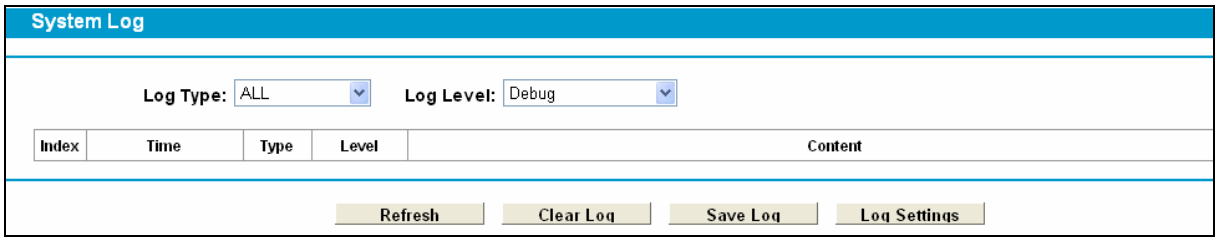


Figure 4-93

- **Log Type:** By selecting the log type, only logs of this type will be shown.
- **Log Level:** By selecting the log level, only logs of this level will be shown.
- **Refresh:** Refresh the page to show the latest log list.
- **Clear Log:** All the logs will be deleted from the Modem Router permanently, not just from the page.
- **Save Log:** Click to save all the logs in a txt file.
- **Log Settings:** Click to set the logs in the screen (shown in Figure 4-94).

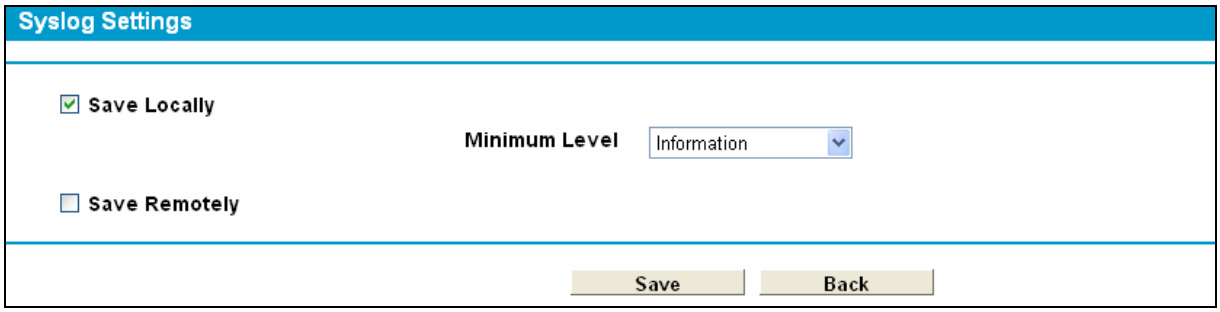


Figure 4-94

- **Save Locally:** If **Save Locally** is selected**,** events will be recorded in the local memory.
- **Minimum Level:** Select the Minimum level in the drop-down list, for the Minimum Level, all logged events above or equal to the selected level will be displayed.
- **Save Remotely:** If **Save Remotely** is selected**,** events will be sent to the specified IP address and UDP port of the remote system log server.

Click the **Save** button to save your settings.

4.17.2 Time Settings

Choose menu "**System Tools**" → "**Time Settings**", and then you can configure the time on the following screen.

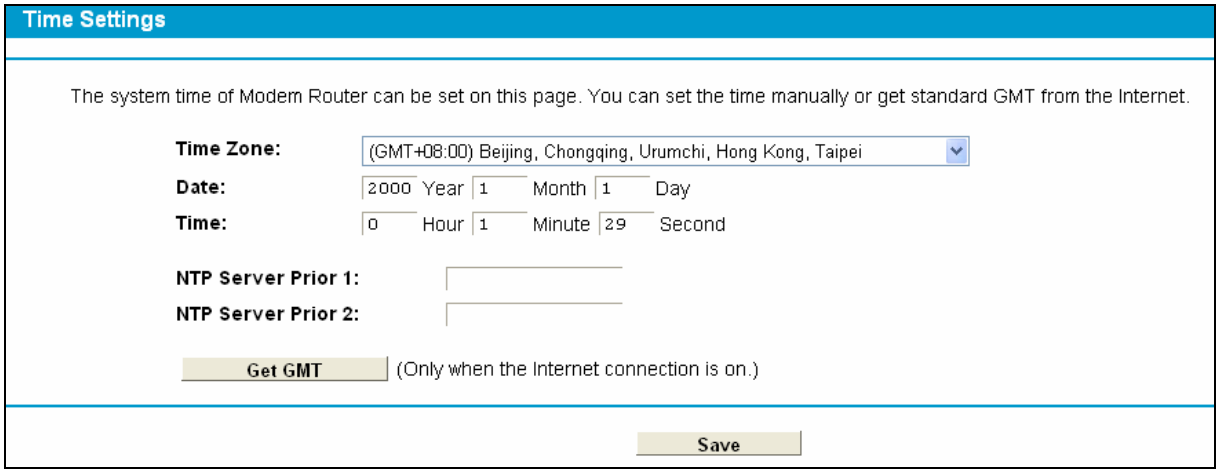

Time Settings
The system time of Modem Router can be set on this page. You can set the time manually or get standard GMT from the Internet.
Time Zone:
(GMT+08:00) Beijing, Chongqing, Urumchi, Hong Kong, Taipei
Date:
2000 Year 1 Month 1 Day
Time:
0 Hour 1 Minute 29 Second
NTP Server Prior 1:
NTP Server Prior 2:
Get GMT
(Only when the Internet connection is on.)
Save

Figure 4-95

- **Time Zone:** Select your local time zone from this pull down list.
- **Date:** Enter your local date in MM/DD/YY into the right blanks.
- **Time:** Enter your local time in HH/MM/SS into the right blanks.
- **NTP Server 1 / NTP Server 2:** Enter the address or domain of the **NTP Server 1** or **NTP Server 2**, and then the Modem Router will get the time from the NTP Server preferentially. In addition, the Modem Router built-in some common NTP Servers, so it can get time automatically once it connects the Internet.

To set time manually:

1. Select your local time zone.
2. Enter the **Date** in Year/Month/Day format.

3. Enter the **Time** in Hour/Minute/Second format.
4. Click **Save**.

To set time automatically:

1. Select your local time zone.
2. Enter the address or domain of the **NTP Server 1** or **NTP Server 2**.
3. Click the **Get GMT** button to get system time from Internet if you have connected to the Internet.

4.17.3 Manage Control

Choose "**System Tools**" → "**Manage Control**", you can see the screen (shown in Figure 4-94)

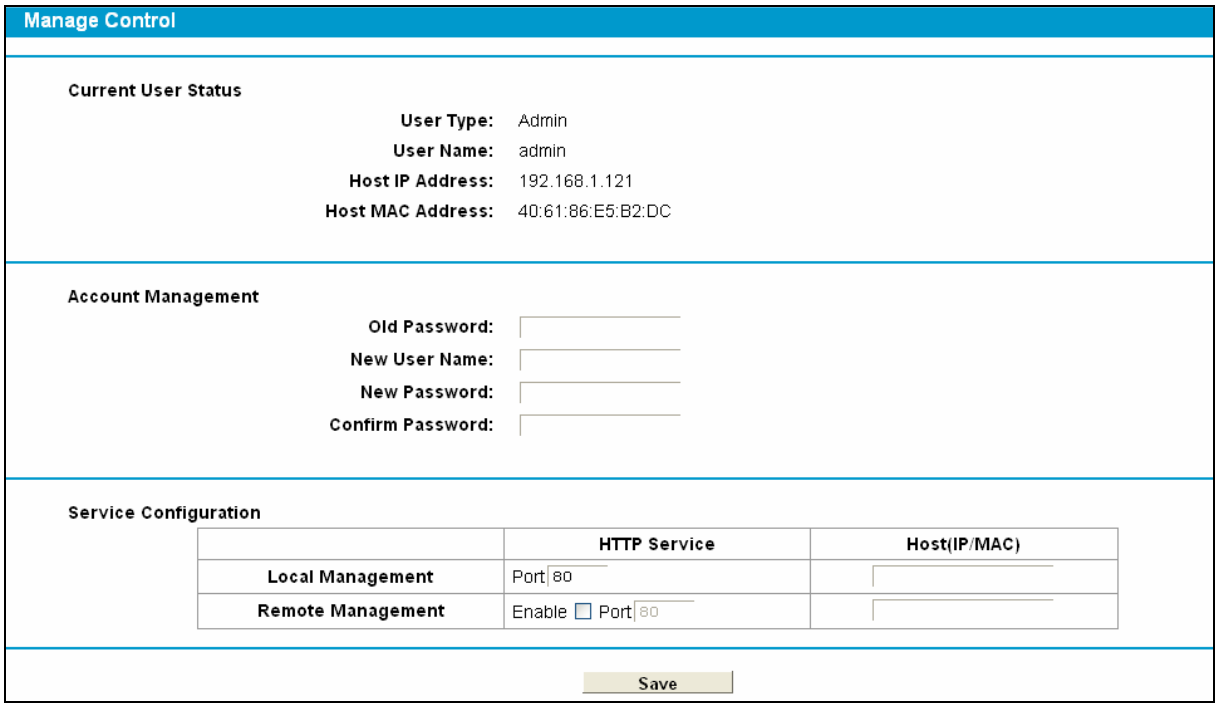


Figure 4-96

- **Current User Status:** This box displays the information about **User Type**, **User Name**, **Host IP Address and Host MAC Address**.
- **Account Management:** Here you can set the account user information about **Old Password**, **New User Name**, **New Password and Confirm Password**.
- **Service Configuration:** Here you can modify the port of the Modem Router's web management interface and limit the hosts which can login this Modem Router's web management interface.

4.17.4 CWMP Settings

Choose "**System Tools**" → "**CWMP Settings**", you can configure the CWMP function in the screen.

The Modem Router offers CWMP feature. The function supports TR-069 protocol which collects information, diagnoses the devices and configures the devices automatically via ACS (Auto-Configuration Server).

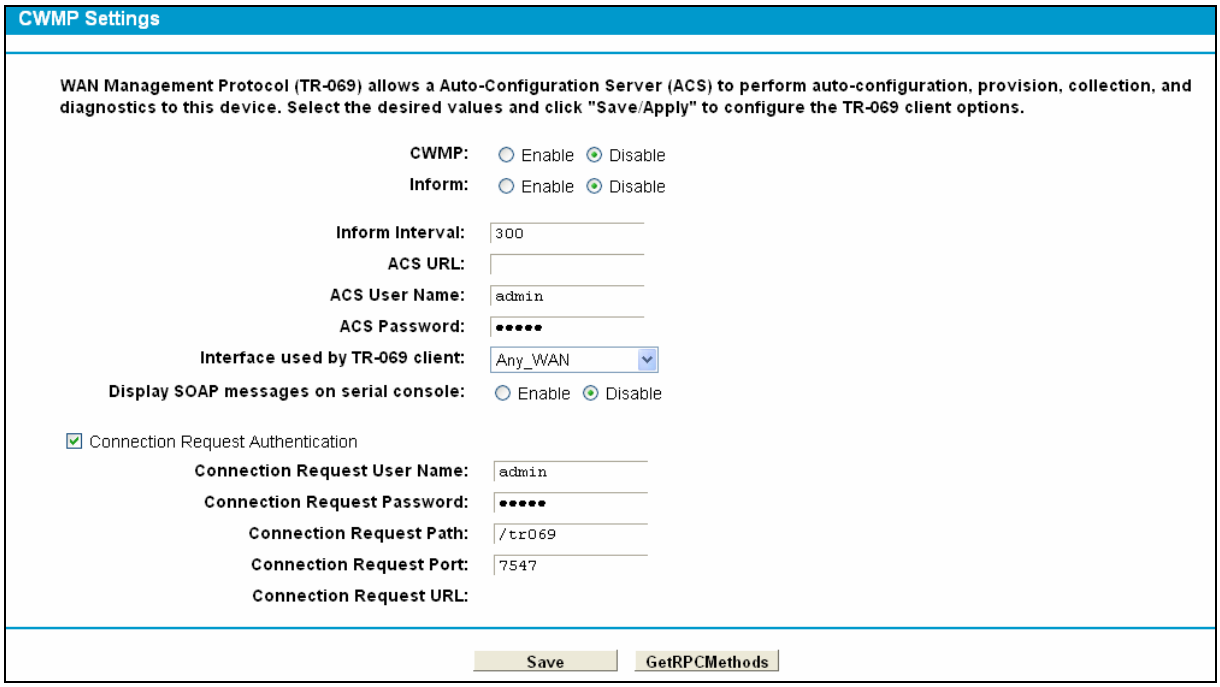

CWMP Settings
WAN Management Protocol (TR-069) allows a Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device. Select the desired values and click "Save/Apply" to configure the TR-069 client options.
CWMP: Enable Disable
Inform: Enable Disable
Inform Interval: 300
ACS URL:
ACS User Name: admin
ACS Password:
Interface used by TR-069 client: Any_WAN
Display SOAP messages on serial console: Enable Disable
Connection Request Authentication
Connection Request User Name: admin
Connection Request Password:
Connection Request Path: /tr069
Connection Request Port: 7547
Connection Request URL:
Save
GetRPCMethods

Figure 4-97

- **CWMP:** Select enable the CWMP function.
- **Inform:** Enable or disable the function. If enabled, the information will be informed to ACS server periodically.
- **Inform Interval:** Enter the interval time here.
- **ACS URL:** Enter the website of ACS which is provided by your ISP.
- **ACS User Name/Password:** Enter the User Name and password to login the ACS server.
- **Interface used by TR-069 client:** Select the interface used by TR-069 client.
- **Display SOAP messages on serial console:** Enable or disable this function.
- **Connection Request User Name/Password:** Enter the User Name and Password that provided the ACS server to login the Modem Router.
- **Connection Request Path:** Enter the path that connects to the ACS server.
- **Connection Request Port:** Enter the port that connects to the ACS server.
- **Connection Request URL:** Enter the URL that connects to the ACS server.

4.17.5 SNMP Settings

Choose "**Management**"→"**SNMP Agent**", you can see the SNMP-Configuration screen as shown below.

SNMP (Simple Network Management Protocol) has been widely applied in the computer networks currently, which is used for ensuring the transmission of the management information between any two nodes. In this way, network administrators can easily search and modify the information on any node on the network. Meanwhile, they can locate faults promptly and implement the fault diagnosis, capacity planning and report generating.

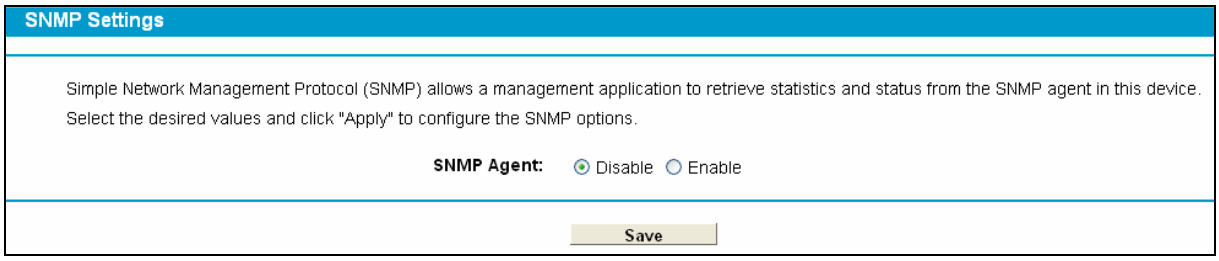

SNMP Settings
Simple Network Management Protocol (SNMP) allows a management application to retrieve statistics and status from the SNMP agent in this device.
Select the desired values and click "Apply" to configure the SNMP options.
SNMP Agent:
Disable
Enable
Save

Figure 4-98

An **SNMP Agent** is an application running on the Modem Router that performs the operational role of receiving and processing SNMP messages, sending responses to the SNMP manager, and sending traps when an event occurs. So a router contains SNMP "agent" software can be monitored and/or controlled by SNMP Manager using SNMP messages.

4.17.6 Backup & Restore

Choose menu "**System Tools**" → "**Backup & Restore**", and then you can save the current configuration of the Modem Router as a backup file and restore the configuration via a backup file as shown in Figure 4-99.

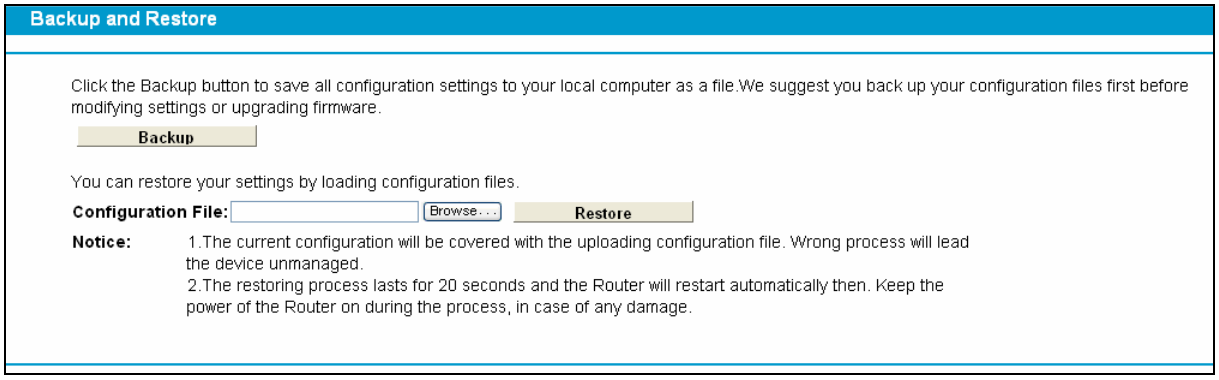

Backup and Restore
Click the Backup button to save all configuration settings to your local computer as a file.We suggest you back up your configuration files first before modifying settings or upgrading firmware.
Backup
You can restore your settings by loading configuration files.
Configuration File:
Browse...
Restore
Notice:
1.The current configuration will be covered with the uploading configuration file. Wrong process will lead the device unmanaged.
2.The restoring process lasts for 20 seconds and the Router will restart automatically then. Keep the power of the Router on during the process, in case of any damage.

Figure 4-99

- Click the **Backup** button to save all configuration settings as a backup file in your local computer.
- To upgrade the Modem Router 's configuration, follow these instructions.
  - Click the **Browse** button to find the configuration file which you want to restore.
  - Click the **Restore** button to update the configuration with the file whose path is the one you have input or selected in the blank.

Note:

The current configuration will be covered with the uploading configuration file. Wrong process will lead the device unmanaged. The restoring process lasts for 20 seconds and the Modem Router will restart automatically then. Keep the power of the Modem Router on during the process, in case of any damage.

4.17.7 Factory Defaults

Choose menu "**System Tools** → **Factory Defaults**", and then and you can restore the configurations of the Modem Router to factory defaults on the following screen

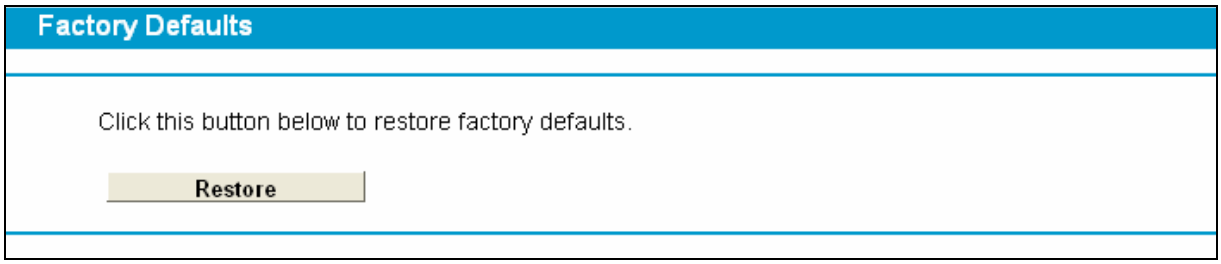


Figure 4-100

Click the **Restore** button to reset all configuration settings to their default values.

- The default **User Name**: admin
- The default **Password**: admin
- The default **Subnet Mask**: 255.255.255.0

Note:

All changed settings will be lost when defaults are restored.

4.17.8 Firmware Upgrade

Choose menu "**System Tools → Firmware Upgrade**", and then you can update the latest version of firmware for the Modem Router on the following screen.

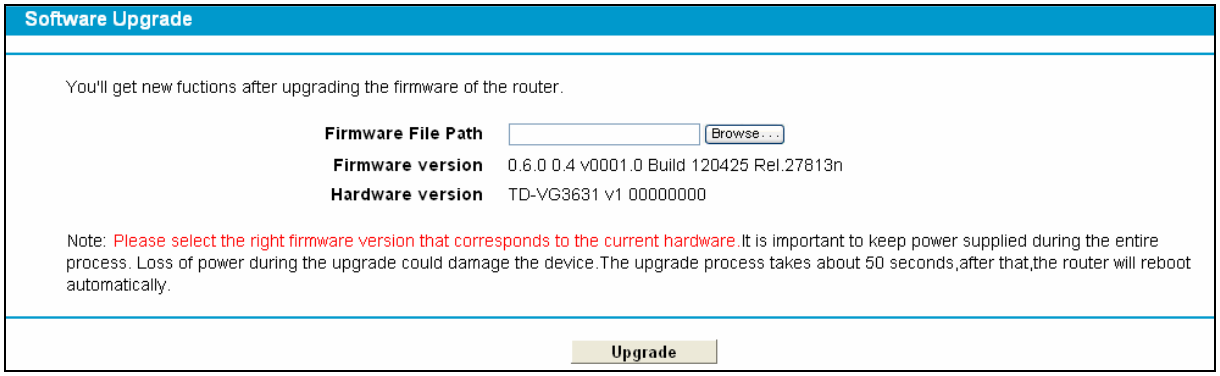

Software Upgrade
You'll get new fuctions after upgrading the firmware of the router.
Firmware File Path
Browse...
Firmware version
0.6.0 0.4 v0001.0 Build 120425 Rel.27813n
Hardware version
TD-VG3631 v1 00000000
Note: Please select the right firmware version that corresponds to the current hardware.It is important to keep power supplied during the entire process. Loss of power during the upgrade could damage the device.The upgrade process takes about 50 seconds,after that,the router will reboot automatically.
Upgrade

Figure 4-101

- **Firmware Version:** Displays the current firmware version.
- **Hardware Version:** Displays the current hardware version. The hardware version of the upgrade file must accord with the Modem Router's current hardware version.

To upgrade the Modem Router's firmware, follow these instructions below:

1) Download a most recent firmware upgrade file from our website (www.tp-link.com).
2) Enter or select the path name where you save the downloaded file on the computer into the **File Name** blank.
3) Click the **Upgrade** button.
4) The Modem Router will reboot while the upgrading has been finished.

Note:

1) New firmware versions are posted at http://www.tp-link.com and can be downloaded for free.

There is no need to upgrade the firmware unless the new firmware has a new feature you want to use. However, when experiencing problems caused by the Modem Router rather than the configuration, you can try to upgrade the firmware.

2) When you upgrade the Modem Router's firmware, you may lose its current configurations, so before upgrading the firmware please write down some of your customized settings to avoid losing important settings.

3) Do not turn off the Modem Router or press the Reset button while the firmware is being upgraded. Loss of power during the upgrade could damage the Modem Router.

4) The firmware version must correspond to the hardware.

5) The upgrade process takes a few moments and the Modem Router restarts automatically when the upgrade is complete.

4.17.9 Reboot

Choose menu "**System Tools**" → "**Reboot**", and then you can click the **Reboot** button to reboot the Modem Router via the next screen.

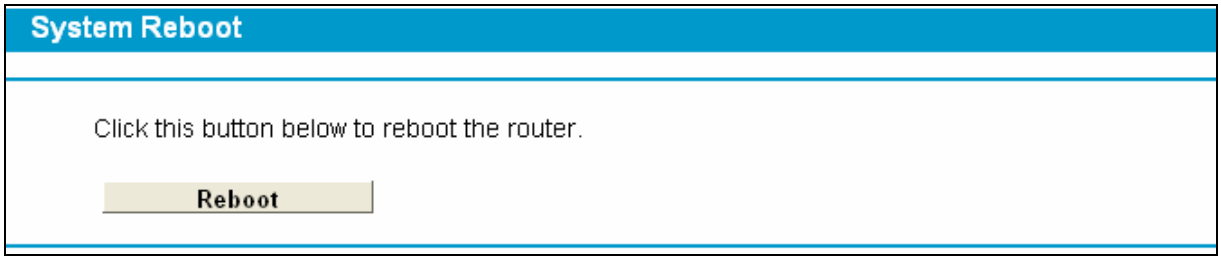


Figure 4-102

Some settings of the Modem Router will take effect only after rebooting, which include

- Change the LAN IP Address (system will reboot automatically).
- Change the DHCP Settings.
- Change the Wireless configurations.
- Change the Web Management Port.
- Upgrade the firmware of the Modem Router (system will reboot automatically).
- Restore the Modem Router's settings to factory defaults (system will reboot automatically).
- Update the configuration with the file (system will reboot automatically.

4.17.10 Statistics

Choose menu "**System Tools**" → "**Statistics**", and then you can view the statistics of the Modem Router, including total traffic and current traffic of the last Packets Statistic Interval.

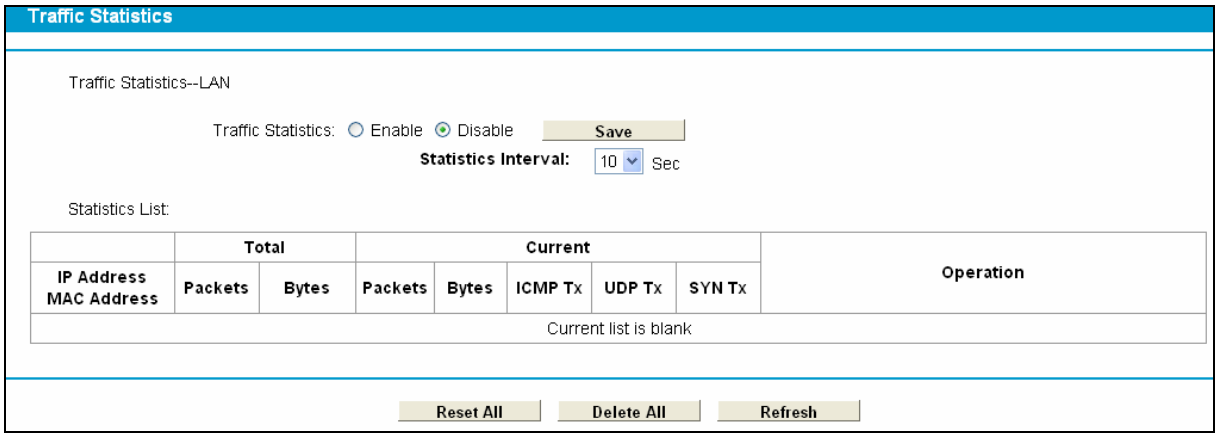


Figure 4-103

- **Statistics Status:** Enable or Disable. The default value is disabled. To enable it, click the **Enable**. If it is disabled, the function of DoS protection in Security settings will be disabled.
- **Statistics Interval (5-60):** The default value is 10. Select a value between 5 and 60 seconds in the drop-down list. The Packets Statistic interval indicates the time section of the packets statistic.

Click **Reset All** to reset the values of all the entries to zero.

Click **Delete All** to delete all entries in the table.

Click the **Refresh** button to refresh immediately.

Statistics Table:

IP/MAC Address		The IP and MAC address are displayed with related statistics.
Total	**Packets**	The total number of packets received and transmitted by the Modem Router.
	Bytes	The total number of bytes received and transmitted by the Modem Router.
Current	**Packets**	The total number of packets received and transmitted in the last Packets Statistic interval seconds.
	Bytes	The total number of bytes received and transmitted in the last Packets Statistic interval seconds.
	ICMP Tx	The number of the ICMP packets transmitted to WAN per second at the specified Packets Statistics interval. It is shown like “current transmitting rate / Max transmitting rate”.
	UDP Tx	The number of UDP packets transmitted to the WAN per second at the specified Packets Statistics interval. It is shown like “current transmitting rate / Max transmitting rate”.
	SYN Tx	The number of TCP SYN packets transmitted to the WAN per second at the specified Packets Statistics interval. It is shown like “current transmitting rate / Max transmitting rate”.
Operation	**Reset**	Reset the value of he entry to zero.
	Delete	Delete the existing entry in the table.

Appendix A: Specifications

General	
Standards and Protocols	ANSI T1.413.I2, ITU G.992.1, ITU G.992.2, ITU G.992.3, ITU G.992.5, IEEE802.1p, IEEE 802.11b,IEEE802.11e, IEEE 802.11g, IEEE 802.11n, IEEE 802.3, IEEE 802.3u, TCP/IP, PPPoA, PPPoE, SNTP, HTTP, DHCP, ICMP, NAT
Safety & Emission	FCC, CE
Ports	Four 10/100M Auto-Negotiation RJ45 ports（Auto MDI/MDIX) Four RJ11 ports Two USB 2.0 ports
LEDs	Power, ADSL, Internet, WLAN, 1,2,3,4(LAN) 1,,2(USB), Line, 1,2(Phone), WPS
Network Medium	10Base-T: UTP category 3, 4, 5 cable 100Base-TX: UTP category-5 Max line length: 6.5Km
Data Rates	Downstream: Up to 24Mbps Upstream: Up to 3.5Mbps（With Annex M enabled）
System Requirement	Internet Explorer 5.0 or later, Netscape Navigator 6.0 or later Win 9x/ ME/ 2000/ XP/ Vista/ 7
Physical and Environment	
Working Temperature	0℃ ~ 40℃
Working Humidity	10% ~ 90% RH (non-condensing)
Storage Temperature	-40℃ ~ 70℃
Storage Humidity	5% ~ 90% RH (non-condensing)

Appendix B: Troubleshooting

T1. How do I restore my Modem Router's configuration to its factory default settings?

With the Modem Router powered on, press and hold the **RESET** button on the front panel for 8 to 10 seconds before releasing it.

☞ **Note**:

Once the Modem Router is reset, the current configuration settings will be lost and you will need to re-configure the router.

T2. What can I do if I don't know or forget my password?

1) Restore the Modem Router's configuration to its factory default settings. If you don't know how to do that, please refer to **T1**.
2) Use the default user name and password: **admin**, **admin**.
3) Try to configure your Modem Router once again by following the instructions in 4.1 Login.

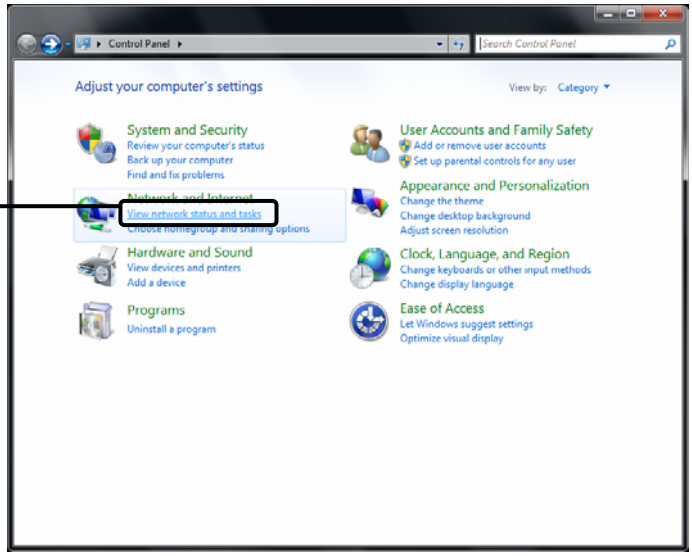
T3. What can I do if I cannot access the web-based configuration page?

1) Configure your computer's IP Address.

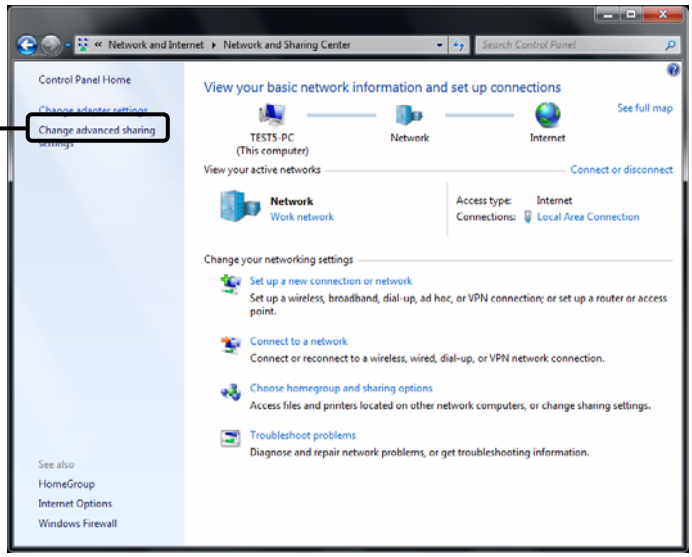
For Windows 7 OS

Go to **Start** > **Settings** > **Control Panel**, and then you will see the following page.

Click **View network status and tasks**

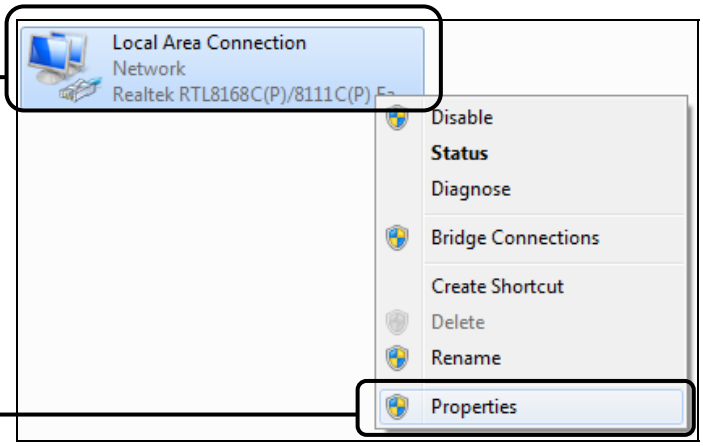


Click **Change adapter settings**

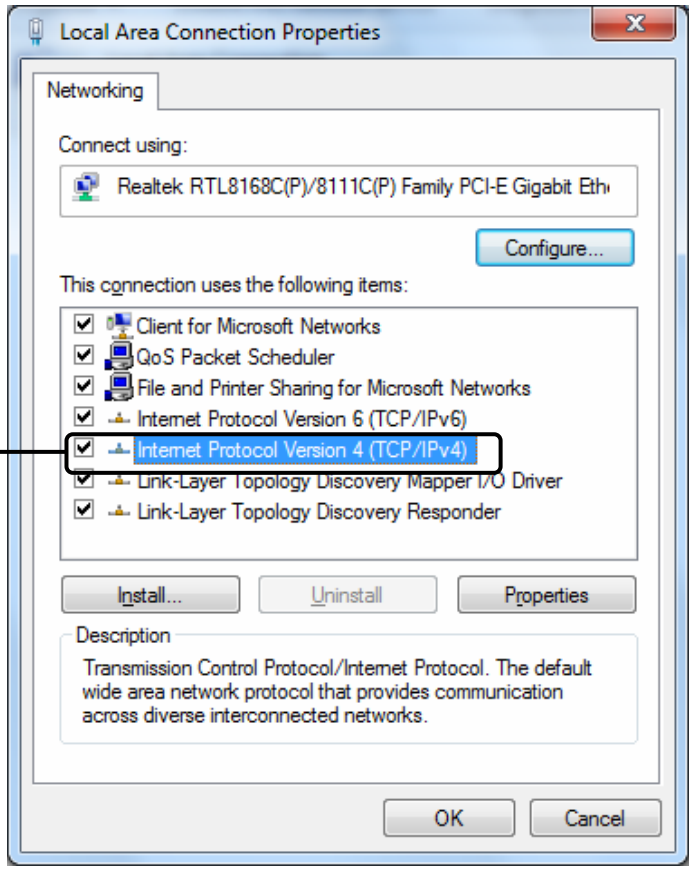

Network and Internet ▸ Network and Sharing Center
Search Control Panel
Control Panel Home
Change advanced sharing
View your basic network information and set up connections
See full map
TEST5-PC
(This computer)
Network
Internet
View your active networks
Connect or disconnect
Network
Work network
Access type: Internet
Connections: Local Area Connection
Change your networking settings
Set up a new connection or network
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.
Connect to a network
Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.
Choose homegroup and sharing options
Access files and printers located on other network computers, or change sharing settings.
Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.
See also
HomeGroup
Internet Options
Windows Firewall

Right-click **Local Area Connection**

Click **Properties**



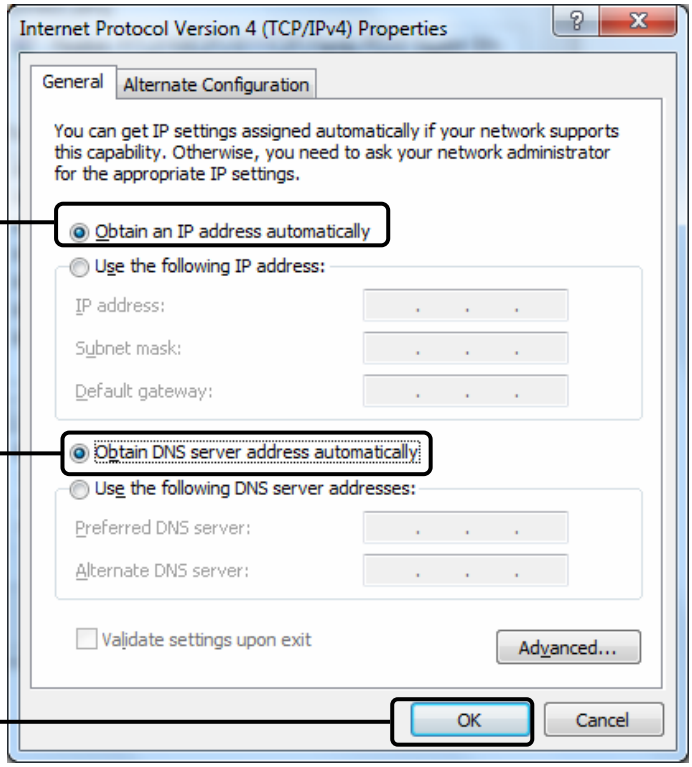
Double-click **Internet Protocol Version 4 (TCP/IPv4)**



Select **Obtain an IP address automatically**

Select **Obtain DNS server address automatically**

Click **OK**

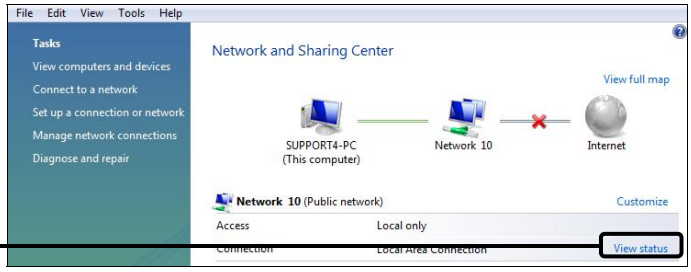

Internet Protocol Version 4 (TCP/IPv4) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Validate settings upon exit
Advanced...
OK
Cancel

For Windows Vista OS

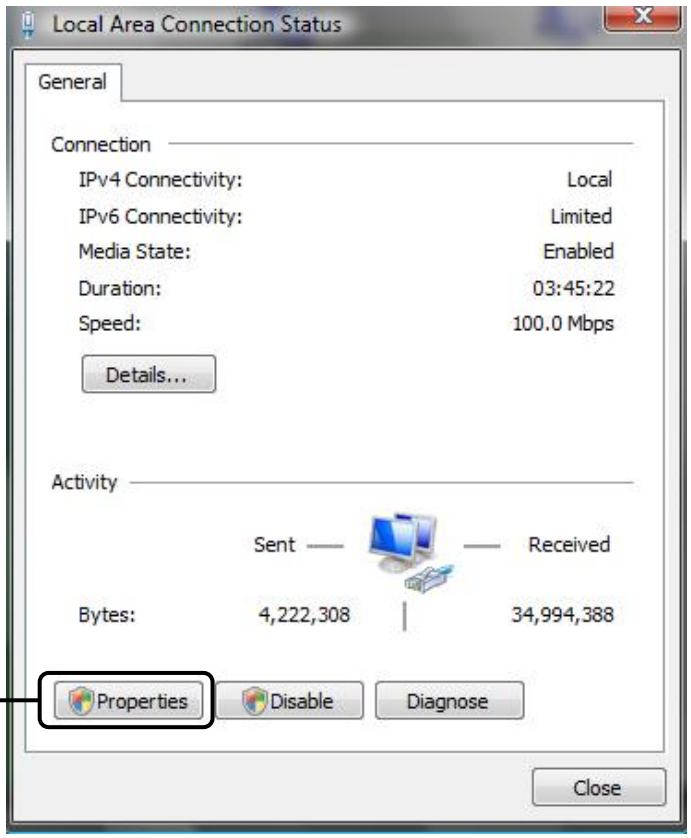
Go to **Start** > **Settings** >**Control Panel**, and then you will see the following page.

Click **View network status and tasks**

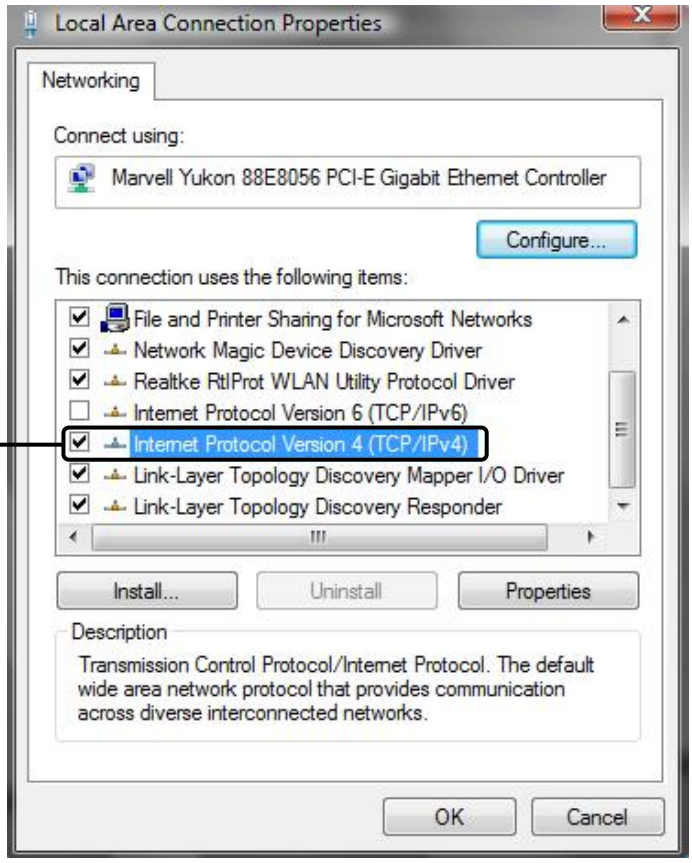
Click **View status**



Click **Properties**



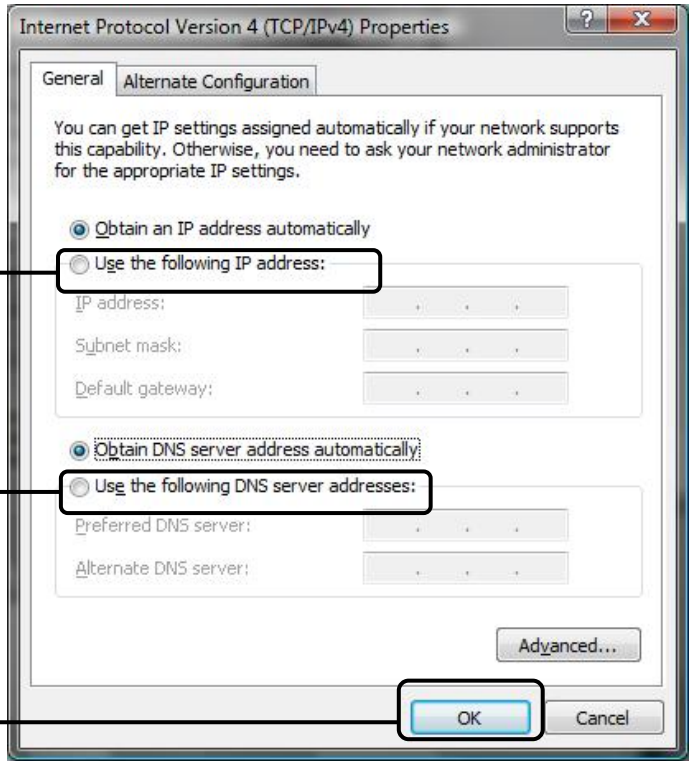
Double-click **Internet Protocol Version 4 (TCP/IPv4)**


Local Area Connection Properties
Networking
Connect using:
Marvell Yukon 88E8056 PCI-E Gigabit Ethernet Controller
Configure...
This connection uses the following items:
File and Printer Sharing for Microsoft Networks
Network Magic Device Discovery Driver
Realtke RtlProt WLAN Utility Protocol Driver
Internet Protocol Version 6 (TCP/IPv6)
Internet Protocol Version 4 (TCP/IPv4)
Link-Layer Topology Discovery Mapper I/O Driver
Link-Layer Topology Discovery Responder
Install...
Uninstall
Properties
Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
OK
Cancel

Select **Obtain an IP address automatically**

Select **Obtain DNS server address automatically**

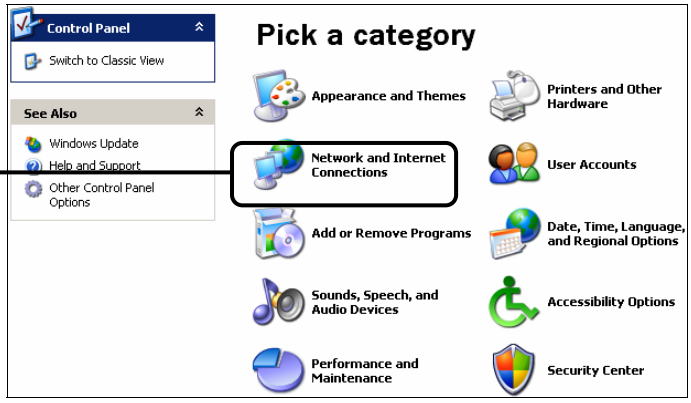
Click **OK**


Internet Protocol Version 4 (TCP/IPv4) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

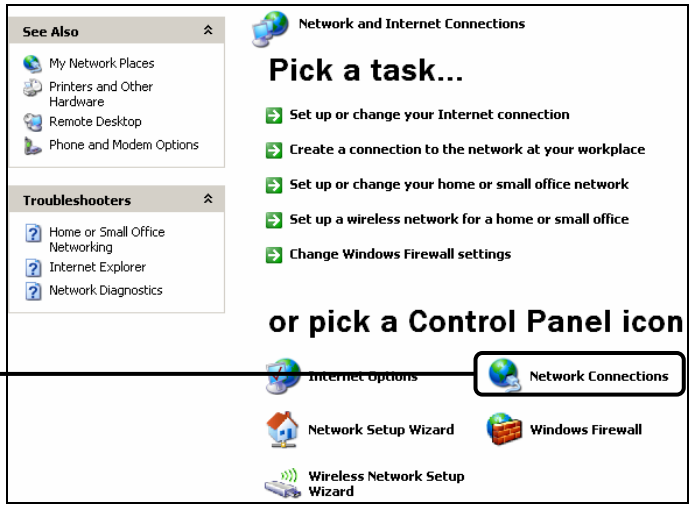
For Windows XP OS

Go to **Start** > **Control Panel**, you will then see the following page.

Click **Network and Internet Connections**

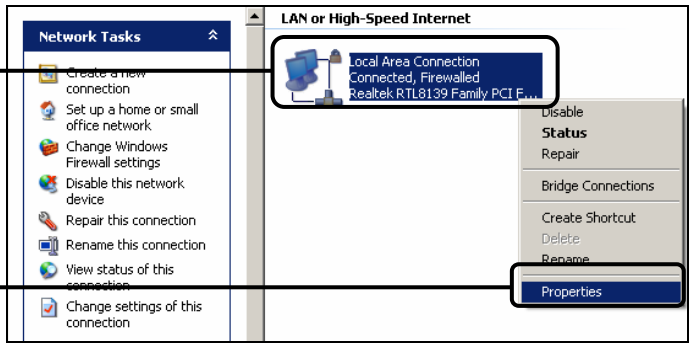


Click **Network Connections**

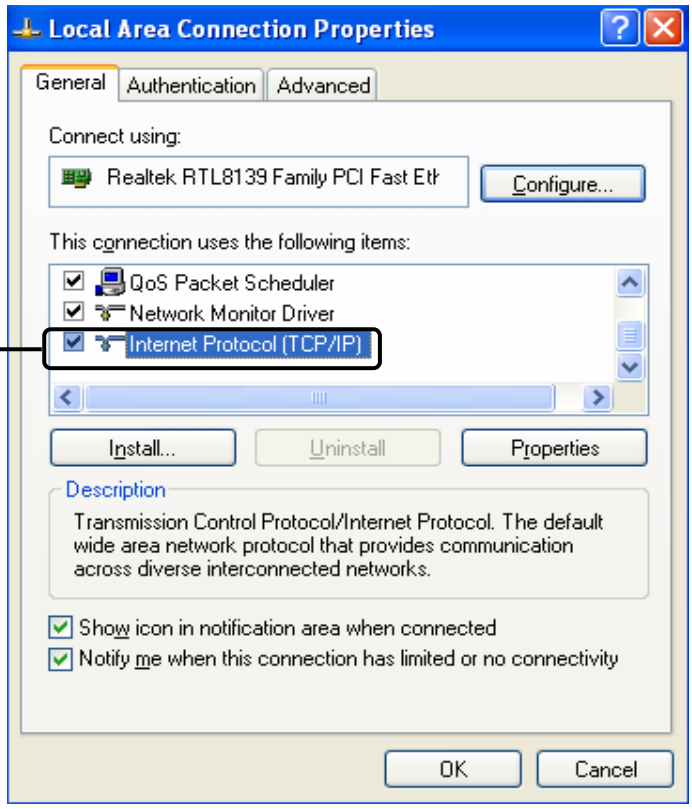

See Also
My Network Places
Printers and Other Hardware
Remote Desktop
Phone and Modem Options
Troubleshooters
Home or Small Office Networking
Internet Explorer
Network Diagnostics
Network and Internet Connections
Pick a task...
Set up or change your Internet connection
Create a connection to the network at your workplace
Set up or change your home or small office network
Set up a wireless network for a home or small office
Change Windows Firewall settings
or pick a Control Panel icon
Internet Options
Network Connections
Network Setup Wizard
Windows Firewall
Wireless Network Setup Wizard

Right-click **Local Area Connection**

Click **Properties**



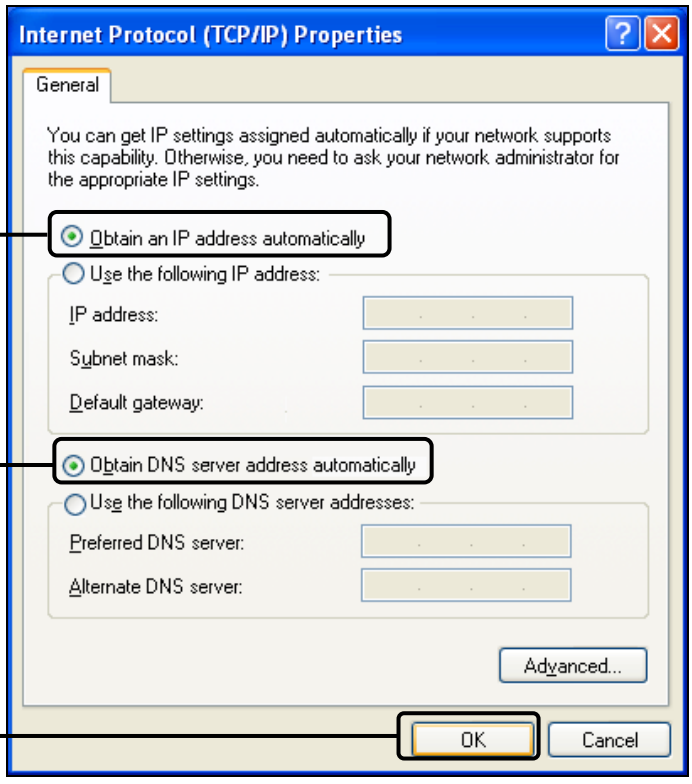
Double-click **Internet Protocol (TCP/IP)**

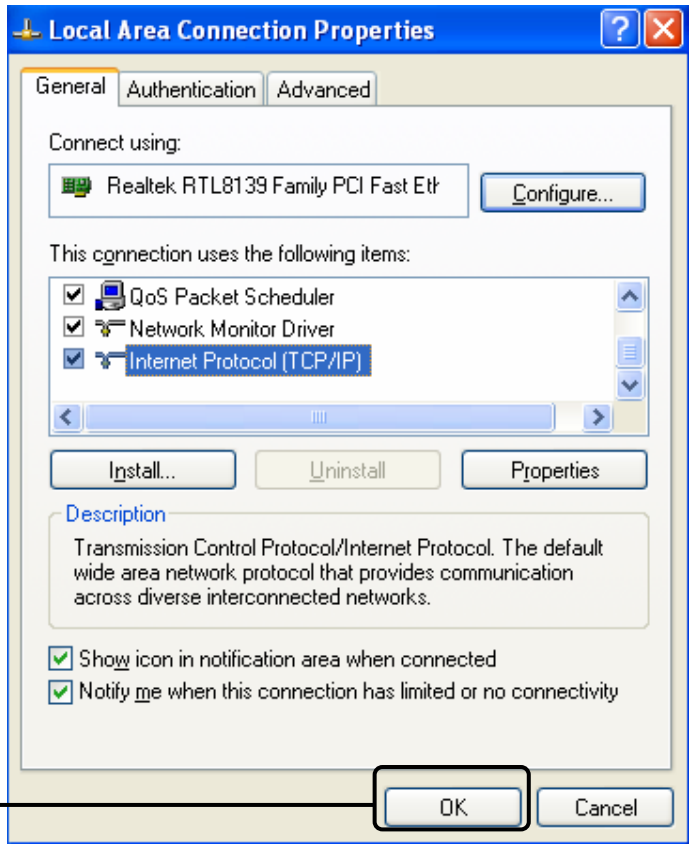


Select **Obtain an IP address automatically**

Select **Obtain DNS server address automatically**

Click **OK**


Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

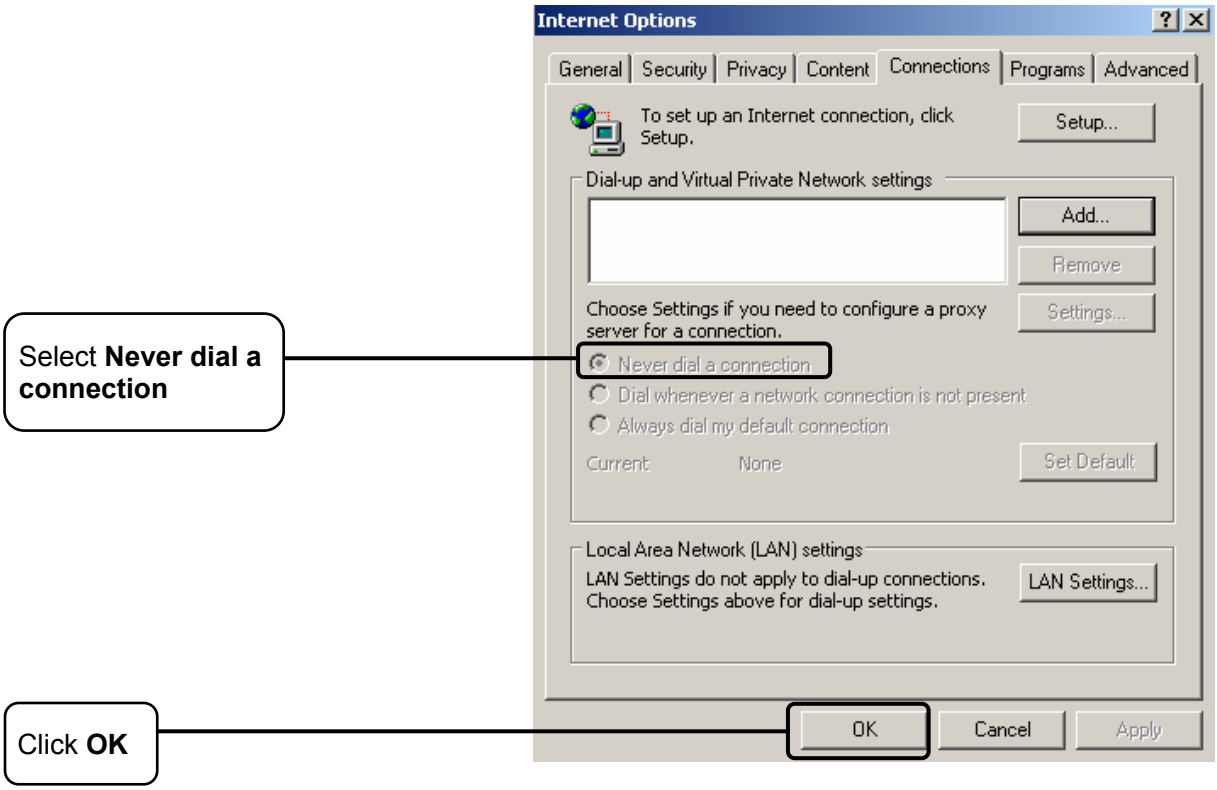


Click **OK**

2) Configure your IE browser

Open your IE browser, click **Tools** tab and you will see the following screen.

Click **Internet Options**



Now, try to log on to the Web-based configuration page again after the above settings have been configured. If you still cannot access the configuration page, please restore your Modem Router's factory default settings and reconfigure your Modem Router following the instructions in 4.1 Login. Please feel free to contact our Technical Support if the problem still exists.

T4. What can I do if I cannot access the Internet?

1) Check to see if all the connectors are connected well, including the telephone line, Ethernet cables and power adapter.
2) Check to see if you can log on to the web management page of the Modem Router. If you can, try the following steps. If you cannot, please set your computer referring to **T3** then try to see if you can access the Internet. If the problem persists, please go to the next step.
3) Consult your ISP and make sure all the VPI/VCI, Connection Type, account username and password are correct. If there are any mistakes, please correct the settings and try again.
4) If you still cannot access the Internet, please restore your Modem Router to its factory default settings and reconfigure your Modem Router by following the instructions in 4.1 Login.
5) Please feel free to contact our Technical Support if the problem still exists.

☞ **Note:**

For more details about Troubleshooting and Technical Support contact information, please log on to our Technical Support Website: **http://www.tp-link.com/en/support**

Appendix C: Telephony Features

Call Holding

This feature allows you to put a call on hold, in which case the call is not ended but no verbal communication is available.

To put a call on hold, press the flash button. To return to the original call, press the flash button again.

Call Transfer

This feature allows you to redirect the current call to another phone by using the flash button and dialing the destination number.

To transfer a call, follow the steps below:

1. Press flash button to put the current call on hold.
2. Dial the destination number.
3. Hang up when hearing the ringback tone or wait for the newly called party to answer and then hang up.
4. To quit the transfer (if the newly called party doesn't answer), press the flash button to return to the original call.

Call Waiting

With this feature enabled, you will hear the call waiting tone during a call. Press flash followed by the number 2 to answer the new incoming call. The first call is automatically put on hold. You can switch between the two calls by pressing flash followed by the number 2.

Three-way Conference Call

This feature allows more than two but at most three people to communicate at the same time.

To make a three-way conference call, follow the steps below:

1. Press the flash button to put the first call on hold.
2. Dial the destination number.
3. Wait for the third party to answer and then press flash +3 to connect the three people together.
4. To drop yourself out of the call, simply hang up.

A three-way conference call can also be set up during a call with the Call Waiting enabled. When hearing the call waiting tone during a call, press flash followed by the number 3 to connect the three people together.

It should be noted that the call will end if the initiator of the three-way conference call hangs up. However, the call will not end if anyone of the other two parties hangs up. The left two parties remain connected to each other.

Call Forwarding

This feature allows an incoming call to be redirected to a specified party. There are three call forwarding features, including Call Forwarding Unconditionally, Call Forwarding on Busy and Call Forwarding on No Answer.

✓ With Call Forwarding Unconditionally enabled, no matter whether the called party is engaged

or not, the incoming call will be redirected to the specified party.

- ✓ With Call Forwarding on Busy enabled, the incoming call will be redirected to the specified party when the called party is engaged.
- ✓ With Call Forward on No Answer enabled, the incoming call will be redirected to the specified party when there is no response for a certain time.

Anonymous Calling

This feature allows you to make a call without your phone number or ID being displayed on the called party's phone.

Anonymous Call Blocking

With this feature enabled, all anonymous calls will be blocked.

Speed Dial

Speed Dial comes to store frequently used telephone numbers and to make your dial more convenient. It allows you to make a call by pressing one or two digits and the key # instead of the original phone number.

Warm Line

With this feature enabled, a call will be automatically redirected to a specified party without taking any additional action when the phone goes off-hook for a certain time.

USB Voice Mail

With this feature enabled, the caller will be prompted to leave a voice message upon the call or when there is no response for a certain time.

DND (Do Not Disturb)

With this feature enabled, all the incoming calls will be blocked and the caller will hear the busy tone.

Appendix D: Telephone Operation

Code	Description	Usage
*20	Listen to voice messages stored in your USB storage device.	Press 0 to listen to new voice messages.
		Press 1 to listen to the previous message.
		Press 2 to listen to the current message again.
		Press 3 to listen to the next message.
		Press 4 to delete the current message.
		Press 5 to listen to all the messages.
*60	Disable Call Waiting.	Pick up the phone to dial this code. After hearing the confirmation tone, hang up to make the configuration take effect.
*61	Enable Call Waiting.	Pick up the phone to dial this code. After hearing the confirmation tone, hang up to make the configuration take effect.
*62	With Call Waiting enabled, disable it for the call you are going to make.	Pick up the phone to dial this code. You will hear the confirmation tone and then the dial tone which will prompt you to dial the destination number.
*63	With Call Waiting disabled, enable it for the call you are going to make.	Pick up the phone to dial this code. You will hear the confirmation tone and then the dial tone which will prompt you to dial the destination number.
*99	Redial on busy.	Pick up the phone to dial this code. You will hear the confirmation tone and then the dial tone which will prompt you to dial the destination number. Hanging up and then picking up your phone again can disable this feature.
*70	Disable all the call forwarding features.	Pick up the phone to dial this code. After hearing the confirmation tone, hang up to make the configuration take effect.
*71	Enable Call Forwarding on No Answer.	Pick up the phone to dial this code. After hearing the confirmation tone, hang up to make the configuration take effect.
*72	Enable Call Forwarding on Busy.	Pick up the phone to dial this code. After hearing the confirmation tone, hang up to make the configuration take effect.

*73	Enable Call Forwarding Unconditionally.	Pick up the phone to dial this code. After hearing the confirmation tone, hang up to make the configuration take effect.
*69	Dial the last incoming number.	Pick up the phone to dial this code. The last incoming number will be dialed automatically.
*68	Dial the last outgoing number.	Pick up the phone to dial this code. The last outgoing number will be dialed automatically.
*78	Enable Warm Line.	Pick up the phone to dial this code. After hearing the confirmation tone, hang up to make the configuration take effect.
*79	Disable Warm Line.	Pick up the phone to dial this code. After hearing the confirmation tone, hang up to make the configuration take effect.
*80	Enable Anonymous Call Blocking.	Pick up your phone to dial this code. After hearing the confirmation tone, hang up to make the configuration take effect.
*81	Disable Anonymous Call Blocking.	Pick up the phone to dial this code. After hearing the confirmation tone, hang up to make the configuration take effect.
*82	With Anonymous Calling disabled, enable it for the call you are going to make.	Pick up the phone to dial this code. You will hear the confirmation tone and then the dial tone which prompts you to dial the destination number.
*83	Enable Anonymous Calling.	Pick up the phone to dial this code. After hearing the confirmation tone, hang up to make the configuration take effect.
*84	Disable Anonymous Calling.	Pick up the phone to dial this code. After hearing the confirmation tone, hang up to make the configuration take effect.
*86	Enable DND.	Pick up the phone to dial this code. After hearing the confirmation tone, hang up to make the configuration take effect.
*87	Disable DND.	Pick up the phone to dial this code. After hearing the confirmation tone, hang up to make the configuration take effect.
*90	With Anonymous Calling enabled, disable it for the call you are going to make.	Pick up the phone to dial this code. You will hear the confirmation tone and then the dial tone which prompts you to dial the destination number.

Appendix E: Technical Support

Technical Support

- For more troubleshooting help, go to:
  www.tp-link.com/support/faq.asp
- To download the latest Firmware, Driver, Utility and User Guide, go to:
  www.tp-link.com/support/download.asp
- For all other technical support, please contact us by using the following details:

Global
Tel: +86 755 26504400
E-mail: support@tp-link.com
Service time: 24hrs, 7 days a week

Singapore
Tel: +65 62840493
E-mail: support.sg@tp-link.com
Service time: 24hrs, 7 days a week

UK
Tel: +44 (0) 845 147 0017
E-mail: support.uk@tp-link.com
Service time: 24hrs, 7 days a week

USA/Canada
Toll Free: +1 866 225 8139
E-mail: support.usa@tp-link.com
Service time: 24hrs, 7 days a week

Malaysia
Tel: 1300 88 875465 (1300 88TPLINK)
Email: support.my@tp-link.com
Service time: 24hrs, 7 days a week

Turkey
Tel: 444 19 25 (Turkish Service）
E-mail: support.tr@tp-link.com
Service time: 9:00 AM to 6:00 PM
7 days a week

Poland
Tel: +48 (0) 801 080 618 / +48 22 7217563 (if calls from mobile phone)
E-mail: support.pl@tp-link.com
Service time: Monday to Friday 9:00 AM to 5:00 PM. GMT+1 or GMT+2 (Daylight Saving Time)

Germany / Austria
Tel: +49 1805 875465 (German Service)
+49 1805 TPLINK
E-mail: support.de@tp-link.com
Fee: 0.14 EUR/min from the German fixed phone network and up to 0.42 EUR/min from mobile phone
Service time: Monday to Friday 9:00 AM to 6:00 PM. GMT+ 1 or GMT+ 2 (Daylight Saving Time in Germany)
*Except bank holidays in Hesse

Australia & New Zealand
Tel: AU 1300 87 5465
NZ 0800 87 5465
E-mail: support@tp-link.com.au
Service time: 24hrs, 7 days a week

Italy
Tel: +39 02 66987799
E-mail: support.it@tp-link.com
Service time: Monday to Friday
9:00 AM to 6:00 PM

Ukrainian
Tel: +380 (44) 590-51-14
E-mail: support.ua@tp-link.com
Service time: Monday to Friday
14:00 PM to 22:00 PM

Brazilian
Toll Free: 0800-770-4337 (Portuguese Service)
E-mail: suporte.br@tp-link.com
Service time: Monday to Saturday
08:00 AM to 08:00 PM

Indonesia
Tel: (+62) 021 6259 135
E-mail : support.id@tp-link.com
Service time : Monday to Friday
9:00 -12:00; 13:00 -18:00
*Except public holidays

Switzerland
Tel: +41 (0) 848 800998 (German Service)
E-mail: support.ch@tp-link.com
Fee: 4-8 Rp/min, depending on rate of different time
Service time: Monday to Friday 9:00 AM to 6:00 PM. GMT+ 1 or GMT+ 2
(Daylight Saving Time)

Russian Federation
Tel: 8 (495) 223-55-60
8 (800) 250-55-60 (toll-free call from any RF region)
E-mail: support.ru@tp-link.com
Service time: From 10:00 to 18:00
(Moscow time)
*Except weekends and holidays in Russian Federation